View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Santa Clara University School of Law

Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 36 | Issue 3 Article 2

4-2-2020

RISKS OF BLOCKCHAIN FOR DATA PROTECTION: A EUROPEAN APPROACH

Jiménez-Gómez, Briseida Sofia

Follow this and additional works at: https://digitalcommons.law.scu.edu/chtlj

 Part of the Intellectual Property Law Commons, and the Science and Technology Law Commons

Recommended Citation

Jiménez-Gómez, Briseida Sofia, *RISKS OF BLOCKCHAIN FOR DATA PROTECTION: A EUROPEAN APPROACH*, 36 SANTA CLARA HIGH TECH. L.J. 281 (2020).
Available at: https://digitalcommons.law.scu.edu/chtlj/vol36/iss3/2

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized editor of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com, pamjadi@scu.edu.

RISKS OF BLOCKCHAIN FOR DATA PROTECTION: A EUROPEAN APPROACH

By Briseida Sofia Jiménez-Gómez[1]

Blockchain has come to revolutionize commerce, driving faster and more efficient transactions. This new technology was born to work in a trustless environment, without any need for trusted intermediaries or supervision by state agencies, leaving a digital print that is mostly public and permanent. Nonetheless, the main problem it presents is that the use of blockchain can interfere with an individual's privacy rights. This article explores the challenges posed by blockchain to data protection. Looking into the characteristics of blockchain will be necessary to explore its advantages and limits, especially from a privacy point of view. Blockchain is a kind of technology that is currently disruptive, but its applications can be modulated and configured in different ways depending on the needs. This article examines the territorial and material scope of the General Data Protection Regulation in order to clarify whether it is applicable to blockchain technologies. The issue of identifiers on a blockchain, the allocation of responsibility to participants, the tension with data subjects' rights and, in particular, the right to erasure are discussed. Some recommendations for reconciling data protection and blockchain technologies are proposed, in particular, projecting the privacy by design principle to blockchain applications. Technological developments should not suppose a deterioration of the rights of individuals. However, some technical solutions entail significant trade-offs, as the case on anonymity in cryptocurrencies illustrates.

[1] Real Colegio Complutense Postdoctoral Fellow at the Harvard Law School Institute for Global Law & Policy. PhD in Law Complutense University (Madrid). LL.M. College of Europe (Brugge).

CONTENTS

I. DATA PROTECTION AS A FUNDAMENTAL RIGHT

Article 8 of the European Charter of Fundamental Rights (EUCFR), which became binding in 2009,[2] states that "[e]veryone has the right to the protection of personal data concerning him or her."[3] It expressly recognized a right to the protection of personal data,[4] but it also set out key data protection principles,[5] and ensured their application via an independent regulatory authority.[6] In this way, the EUCFR distinguished the right to data protection from the right to privacy, departing from other human rights instruments such as the European Convention of Human Rights (ECHR).[7] However, as the Court of Justice of the European Union (CJEU) underlined in the *Digital Rights Ireland* case, the two rights are connected.[8] Accordingly, case law of the European Court of Human Rights (ECtHR) on Article 8 of ECHR in relation to data protection remains relevant for the purpose of the interpretation of Article 8 of EUCFR.

Moreover, Article 16 of Treaty on the Functioning of the European Union (TFEU) incorporated "the right to the protection of personal data,"[9] adding a new legal basis for the regulation and reinforcement of data protection in the European Union. The current European approach is defined by the General Data Protection Regulation (GDPR), which empowers data subjects by providing them with rights vis-à-vis data controllers and processors.[10] GDPR establishes a series of rights for data subjects: the right to access collected personal data,[11] the right to rectification,[12] the right to erasure,[13] the right to restriction of processing,[14] the right to data

---

[2] *The protection of fundamental rights in the EU*, FACT SHEETS ON THE EUR. UNION, https://www.europarl.europa.eu/factsheets/en/sheet/146/the-protection-of-fundamental-rights-in-the-eu.

[3] Charter of Fundamental Rights of the European Union, art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 10 [hereinafter EUCFR]. *See generally* Consolidated Version of The Treaty on European Union art. 6(1), Oct. 26, 2012, 2012 O.J. (C 326) 13 [hereinafter TFEU].

[4] *Id*. art. 8(1).

[5] *Id.* art. 8(2).

[6] *Id.* art. 8(3).

[7] Herke Kranenborg, *Article 8 – Protection of Personal Data*, *in* THE EU CHARTER OF FUNDAMENTAL RIGHTS: A COMMENTARY 223, 228 (Steve Peers et al. eds., 2014).

[8] *See* Joined Cases C-293 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine & Nat. Res., Minister for Justice, Equal. & Law Reform, The Comm'r of the Garda Síochána, Ireland & the Att'y Gen., and Kärtner Landesregierung, Micharl Seitlinger, Christof Tschohl & Others, 2014 EUR-Lex CELEX 62012CA0293, ¶ 53 (Apr. 8, 2014) [hereinafter Digital Rights Ireland].

[9] TFEU*, supra* note 3, art. 16(1).

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 4 [hereinafter GDPR].

[11] *See id.* art. 12–14.

[12] *Id.* art. 16.

[13] *Id.* art. 17.

portability,[15] the right to object to processing of personal data,[16] and rights related to automated decision-making and profiling.[17]

This fundamental protection nevertheless is not absolute, since the right to data protection must be weighed frequently with other fundamental rights, such as freedom of expression, the right to inform, and intellectual property rights, among others.[18] This weighing must be carried out under the principle of proportionality. Naturally, these concerns may be resolved differently in various national courts, the CJEU or the ECtHR. In any case, casuistic analysis is required to such an extent that national weighing standards within the European Union itself do not have to coincide, based on Article 85 GDPR in relation to reconcile freedom of expression and information with data privacy.[19]

In some cases, the right to data protection is limited to those located in the European Union, even though it may be considered a human right.[20] Perspectives in the world regarding the right to data protection are not uniform, nor are they expected to be. Recent laws, such as the California Consumer Privacy Act,[21] reflect the desire for greater data protection based on European influences, and even international treaties like the Council of Europe Convention 108[22] have been revised in order to take the adoption of the GDPR into account.[23] Nevertheless, these advances do not employ a common framework about users' rights to their data, in particular, the necessity of a legal basis for processing personal data or (more controversially) the right to be forgotten.

According to Commissioner for Digital Economy and Society, Mariya Gabriel:

---

[14] *Id.* art. 18.
[15] *Id.* art. 20.
[16] GDPR, *supra* note 10, art. 21.
[17] *Id.* art. 22.
[18] *See id.* ¶ 4.
[19] *See id.* ¶ 153.
[20] *See infra* § III.
[21] *See generally* California Consumer Privacy Act, S.B. 1121, 2018 Leg. (Cal. 2018).
[22] *See generally* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 [hereinafter Convention 108].
[23] There has been a symbiotic relationship between the instruments adopted at international level, in particular, the Convention 108, which served as a source of inspiration for European Union Commission to formulate Directive 95/46. *See generally* Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive]. Not surprisingly, Convention 108 influenced policy and legislation far beyond Europe. In the European Union, one of the objectives of Directive 95/46 was to specify and expand the principles and rights of the Convention 108. *Id.* ¶ 11. In 2018, the Council of Europe later revised Convention 108 by a protocol incorporating the GDPR. GDPR, *supra* note 10. The Protocol was adopted by the Committee of Ministers on 18 May 2018. See Decision of the Committee of Ministers, 128th session of the Committee of Ministers, Elsinore, 18 May 2018, www.coe.int/dataprotection

> In the future, all public services will use blockchain technology, Blockchain is a great opportunity for Europe and Member States to rethink their information systems, to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, benefiting citizens, public services and companies.[24]

The European Commission has made evident efforts to promote the use of blockchain. First, launching the E.U. Blockchain Observatory and Forum in February 2018, and second, unsurprisingly, investing more than EUR 80 million in projects to enhance and support the use of blockchain in a wide range of areas, with a view of dedicating approximately EUR 300 million more to blockchain by 2020.[25]

Blockchain technologies entail fundamentally novel privacy concerns that legal scholars must address. Despite the relatively recent adoption of GDPR which took effect on May 25, 2018,[26] the regulation did not consider blockchain technology specifically. How then, will data protection concerns be balanced against the use of blockchain technologies? Technology cannot be isolated from economics and society when the reality is that technology is the result of a human mind. Consequently, the use of blockchain cannot operate on the outskirts of the law. GDPR takes a neutral approach, because it does not target a specific class of technology, but applies to new technologies in general. In this sense, a study addressing the difficulties that blockchain poses to data protection does not recommend a revision of the GDPR, but rather more regulatory guidance with regard to how concepts must be applied in a blockchain context.[27]

This article seeks to contribute to the literature on the interplay between data protection and blockchain technology. Blockchain seems to be incompatible with many of the principles related to data protection that are part of the E.U. acquis. However, it should be noted that the blockchain is a kind of technology that is currently disruptive, but its applications can be modulated and configured in different ways depending on the needs of natural persons and organizations. In fact, the key question would be to know if an organization, whether public or private, needs a blockchain.

---

[24] *European countries join Blockchain Partnership*, EUR. COMMISSION (Apr. 10, 2018), https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership.

[25] *Id*.

[26] GDPR, *supra* note 10, art. 99.

[27] Michèle Finck, *Blockchain and the General Data Protection Regulation*, EUR. PARLIAMENTARY RES. SERV. 97 (July 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

Depending on the organization's private or public sector status and mission, it may be appropriate or harmful to implement blockchain technology.

Section II of this article describes background about blockchain that it is relevant to privacy law. Section III examines the territorial scope of the GDPR. Section IV discusses the problem of identifiers in blockchain and the risk of re-identification of data subjects. Section V analyzes the concept of data controllers with respect to participants in a blockchain platform. Section VI interprets the fundamental right to be forgotten in the context of a blockchain platform. Section VII envisions different strategies for reconciling blockchain platforms and GDPR. Finally, the last section expresses some concluding remarks on the relation of blockchain and data protection.

II. EXPLORING BLOCKCHAIN TECHNOLOGIES

A. Basics of Blockchain Terminology

Blockchain is a new global resource,[28] a way of communicating and storing information in a system without the need of a middleman. The term "blockchain" relates to how data is stored on a ledger. Blockchain is defined as a "type of database: a structured collection of information" where it is essential the use of cryptographic functions to achieve two goals: data integrity and data identity.[29] Instead of storing data in an individual manner, data is encrypted and collected on a block using cryptographic techniques.[30] Then, there are two types of keys used to encrypt or decrypt data depending on the sender and receiver of the information.[31] Normally, the message is encrypted with a private key known only to the sender and the receiver can decrypt it using a public key provided by the sender.[32]

A ledger is a "place" to record all transactions that happen in the system.[33] It is similar to an accounting book or record of the operations carried out, that act as a type of database with the information organized in a certain way. One property of the ledger of most blockchain technologies is immutability, which is considered essential for data integrity. Users are allowed to enter new transactions but not to modify or delete what has been

---

[28] Don Tapscott & Alex Tapscott, *Realizing the Potential of Blockchain* 5 (World Econ. F., White Paper, 2017), http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf.

[29] Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers*, 25 RICH. J.L. & TECH. 1, 5–6 (2018).

[30] Arvind Narayanan & Jeremy Clark, *Bitcoin's Academic Pedigree*, 60 COMM. OF THE ACM 38 (Dec. 2017).

[31] *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C § 1.1 (John Wiley & Sons, 1996).

[32] Bacon et al., *supra* note 29, at 14.

[33] Narayanan & Clark, *supra* note 30, at 36.

entered because it is "append only."[34] On the other hand, information gathers in blocks. Each block is linked to the previous block and it is verified with a timestamp[35]. Blocks are separately encrypted and stored in a chronological order creating the chain.[36]

Besides, it is possible to obtain a succinct cryptographic digest, which is a short string that prevent storing the whole ledger. Consequently, any manipulation of the ledger would be reflected in the cryptographic digest.[37]

A blockchain is a network of nodes, where nodes are responsible to act as a point of communication that can carry out different functions. Nodes on the network can communicate directly with each other. Generally, a node is a point where it is possible to receive, send or create a message.[38] The information is collectively stored in a peer-to-peer network, so the communication infrastructure is distributed and not centralized.[39] All nodes are connected creating a global data structure. There are two kind of nodes depending on the role to play: participating nodes and validating nodes.[40] Participating nodes store synchronized copies of the data meanwhile validating nodes are allowed to add data to the ledger, in accordance with a consensus mechanism based on an agreed-upon algorithm.[41] Validating nodes have computing power and software to validate transactions. Moreover, participating nodes can be full nodes or lightweight nodes depending on how much data are stored by them.[42] Nodes that store an entire copy of all data are full nodes, ensuring the security and correctness of the data.[43] In contrast, a lightweight node appears when a user is connected to a participating node but, in order to add data, it needs to connect to a full node

---

[34] *Id.* at 37.
[35] *Id.* at 38.
[36] *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 23 (Harv. U. Press, 2018).
[37] Narayanan & Clark, *supra* note 30*,* at 38.
[38] *Blockchain and the GDPR*, EUR. UNION BLOCKCHAIN OBSERVATORY AND F. 33 (Oct. 16, 2018), https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true [hereinafter EU BLOCKCHAIN].
[39] Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1371 (2018).
[40] EU BLOCKCHAIN, *supra* note 38, at 14.
[41] Archana Prashanth Joshi et al., *A survey on security and privacy issues of blockchain technology*, 1 MATHEMATICAL FOUND. OF COMPUTING 121, §§ 2.2, 2.4 (May 2018), https://www.aimsciences.org/article/doi/10.3934/mfc.2018007.
[42] John Evans, *Blockchain Nodes: An In-Depth Guide*, NODES.COM, https://nodes.com (last visited March 19, 2020).
[43] *Id.* The author further categorizes full nodes as pruned or archival nodes. *Id.* When pruned full nodes reach the set limit, they retain only their headers and chain placement, and deletes the oldest ones. *Id.* Archival nodes maintain the full blockchain in the database. *Id.*

that synchronizes with the current state of the network.[44] Thus, lightweight nodes do not require so many resources at the expense of security.

B. Classification of Blockchain Technologies

Blockchain technologies can be classified in terms of how access and adding information is structured. There are public or private blockchains and permissioned or permissionless blockchains. First, a public blockchain means that everyone can access to the network, in opposition to a private blockchain where only a certain set of individuals has access to the network.[45] Parties in a private blockchain are often members of a group or they will have to be authorized.[46] Second, blockchain classification is based on who can add information to the network. When anyone can post to the network, the blockchain is called permissionless.[47] Popular public and permissionless blockchains are Bitcoin and Ethereum. By contrast, a permissioned blockchain only allows an individual to add to the network prior to an authorization.[48]

With public and non-permissioned blockchain applications, all parties can download the open source software and participating in the network, without asking prior permission and need to reveal true identity. Therefore, from a data protection perspective, it is not indifferent setting up a public and permissionless blockchain. For example, all data are on Bitcoin's blockchain, except the owners' identities.[49] The content of a document is hashed through a hash function. The result of the hash function is a string of digits to the input data called hash value.[50] The block header is composed by the hash of the previous block, timestamp and other metadata information.[51] This information is public and creates automatic proof of the position and ownership of each block of the chain.[52] In principle, the private key is required, which it is not stored on the ledger but rather in the owner's wallet. However, anybody can see who owns each block because of the block header so it is possible to go through the chain following the links.[53]

---

[44] *Id.*
[45] Rebecca Lewis et al., *Blockchain and Financial Market Innovation*, FED. RES. BANK OF CHICAGO (2017), https://www.chicagofed.org/publications/economic-perspectives/2017/7.
[46] Joshi et al., *supra* note 41, § 2.1.5.
[47] EU BLOCKCHAIN, *supra* note 38, at 14.
[48] *Id.* at 14–15.
[49] However, it is possible to discern the identities of the Bitcoin accounts and even the financial transaction histories. DE FILIPPI & WRIGHT, *supra* note 36, at 68.
[50] Bacon et al., *supra* note 29, at 9.
[51] *Id.* at 12-13. *See also* Joshi et al., *supra* note 41, § 2.3.
[52] Jude Umeh, *Blockchain Double Bubble or Double Trouble?,* 58 ITNOW 59 (2016).
[53] *Id*.

With public and permissioned blockchains applications, anyone can gain access to the network, but authorization is necessary to be able to add information. The Alastria Project in Spain is an example of this type of network.[54] It is the first multisectoral consortium promoted by companies and institutions for the establishment of a semi-public blockchain infrastructure. The mentioned project supports services with legal effectiveness in the Spanish sphere and in accordance with European regulation.[55]

Private and permissioned blockchains are suitable for companies in highly regulated industries, such as banking and financial institutions. In permissioned blockchain applications, an authority or consortium decides who can engage in recording information to the shared database.[56] Therefore, allocating responsibility may be easier because the consortium or central authority ultimately retains control and sets limits on who can access. For instance, the Ripple protocol, which is used by banks, relies on a network of selected participants that validates transactions records.[57] Private and permissioned blockchain applications tend to be faster than public, as the mechanism for consensus is not based in Proof-of-Work, but Proof-of-Stake, and the group of participants may be smaller than in permissionless blockchains.[58] The distinction between Proof-of-Work and Proof-of-Stake comes from how transactions are validated.[59] A miner is a node that calculate hash values. Every node in the network calculates the hash value in PoW.[60] Miners add a random number, called a nonce, to the header of the block in order to create a valid block.[61] In contrast, a PoS protocol entails that miners can mine or validate transactions in a block depending on the amount of the

---

[54] *See* ALASTRIA: ASOCIACIÓN DE TECNOLOGÍAS DESCENTRALIZADAS/BLOCKCHAIN (2019), https://alastria.io/wp-content/uploads/2019/07/2019-07-11_Alastria-Presentación-corporativa_v00.10-2.pdf.

[55] *Id.* Some towns and regions are using blockchain to facilitate administrative procedure. *Id.* At local level, Alcobendas in Madrid and at regional level, Xunta de Galicia can be mentioned. *Id.*

[56] Lewis et al., *supra* note 45.

[57] Vitalik Buterin, *Introducing Ripple: A Detailed Look at Cryptocurrency's New Kid on the Block*, BITCOIN MAGAZINE (Feb. 26, 2013), https://bitcoinmagazine.com/articles/introducing-ripple.

[58] Toshendra K. Sharma, *Advantages and disadvantages of permissionless blockchain*, BLOCKCHAIN COUNCIL (Oct. 3, 2018), https://www.blockchain-council.org/blockchain/advantages-and-disadvantages-of-permissionless-blockchain/.

[59] *Proof of Work vs Proof of Stake*, BITDEGREE (Jan. 9, 2020), https://www.bitdegree.org/tutorials/proof-of-work-vs-proof-of-stake/ (This tutorial considers that the miner who finally gets the reward is the one who has the most powerful/quantity of hardware devices in PoW; while in PoS the model randomly chooses the winner based on the amount they have staked.)

[60] *Id.*

[61] Bacon et al., *supra* note 29, at 24.

base cryptocurrency the user holds.[62] PoS can save electricity costs and allow faster blockchains potentially depending on the specific algorithm.[63] Moreover, miners in PoS earn a transaction fee based on their contribution to the network by freezing their coins as a deposit. Therefore, the reward is a transaction fee proportionately to the amount they have invested.[64]

However, there are also some drawbacks in terms of security because permissioned blockchains may be more vulnerable, since the network relies on selected parties that could be an objective for hackers or parties could collude to tamper the blockchain.[65]

This distinction is important for dealing with privacy issues. On one hand, a permissionless blockchain is usually public when there are no identity restrictions for participation, and anyone can participate without an approval from a gatekeeper. At the same time, a participant can view transaction data and download the entire ledger where all transactions are tracked. According to the mysterious Satoshi Nakamoto, this system creates a new privacy model similar to the level of information released by stock exchanges.[66] This contrasts with the traditional privacy model, where access to transaction data is only allowed to the involved parties and a trusted third party. The transparency of the system is a point of concern, because transactions data are not only available to participants in the network, but also, according to BlockExplorer,[67] to anyone else. Therefore, the *quid pro quo* exists, as a more transparent network undermines privacy.

On the other hand, a permissioned blockchain is inherently private because a participant needs acceptance of the administrator to join the network.[68] The function of the administrator is similar to a gatekeeper. In these systems, not everyone can see the transactions data; only the participants that belong to the network.[69] From a privacy point of view, adjusting a permissioned blockchain may be a solution to comply with most of data protection rules. Indeed, private and permissioned blockchains are usually designed for a specific purpose, in contrast to public blockchains that

---

[62] Joshi et al., *supra* note 41, §2.4.
[63] Vitalik Buterin, *On Stake*, ETHEREUM BLOG (July 5, 2014), https://blog.ethereum.org/2014/07/05/stake/
[64] *See* BITDEGREE, *supra* note 59.
[65] DE FILIPPI & WRIGHT, *supra* note 36, at 30.
[66] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 6, https://bitcoin.org/bitcoin.pdf (last visited Jan. 26, 2020).
[67] BLOCKEXPLORER, https://blockexplorer.com (last visited Mar. 25, 2020).
[68] Lewis et al., *supra* note 45 ("Permissioned blockchains allow certain members to control the confirmation of transactions. These permissioning members (consensus authorities) can exert control in various ways depending upon the network design. They could be responsible for explicitly approving transactions. Another option would be to designate the permissioning members as the sole members of the network able to participate in a cryptographic consensus mechanism.")
[69] *Id.*

tend to serve a general objective. Permissioned blockchains can be helpful for internal use of specific companies or group of companies, for example, to manage their client base. But we should highlight that so far, the most well-known application of blockchain is related to cryptocurrencies and their protocols are run on public networks. The truly innovative blockchain technology rely on those applications that are public and permissionless.[70]

Based on the previous considerations, blockchains do not have certain characteristics a priori, but those that are determined by its developers.

C. Applications of Blockchain

Distributed ledgers are driving disintermediation of traditional intermediaries, resulting in efficient and speedy transactions, lower transaction costs, and enhanced market access.[71] Blockchain can be a solution to some problems that our world encounters, *inter alia*, the problem of identity theft as blockchain technology provides an immutable and secure system; crashes of any server given that blockchain can also allow cloud storage at different geographical points; inefficiencies of logistics management, because it improves monitoring of production or supervision of food chains;[72] simplifying payments in interbank payments with centrally issued cryptocurrencies; reducing costs and time of interpretation of certain "contracts," known as smart-contracts,[73] as these agreements can be fulfilled automatically when they materialize through a computer program and their compliance is not subject to the interpretation of any of the parties.[74]

Cryptocurrencies are the most famous applications of blockchain technology. They could serve to transfer money abroad, in principle, reducing the fees of exchanging in foreign currencies. Another promising application appears to be the Singapore-based AirCarbon Exchange, which

---

[70] DE FILIPPI & WRIGHT, *supra* note 36, at 32.

[71] Zetzsche et al., *supra* note 39, at 1367. For a discussion on applying blockchain to bills of lading, see Naomi Chetrit et al., *Not Just for Illicity Trade in Contraband Anymore: Using Blockchain to Solve a Millennial-Long Problem with Bills of Lading*, 22 VA. J.L. & TECH. [ii] (2018).

[72] *See* Adrien Ogee & Soichi Furuya, *Blockchain is becoming key for global trade - but is that a gift for hackers?*, WORLD ECON. F. (Dec. 11, 2019), https://www.weforum.org/agenda/2019/12/supply-chains-blockchain-cybersecurity-technology/ ("In the supply chain industry alone, distributed ledger technologies are expected to represent close to $10 billion by 2025, up from $93 million in 2017.").

[73] Nick Szabo, *Smart Contracts,* PHONETIC SCI., AMSTERDAM (1994), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[74] *See* Philip Boucher et al., *How Blockchain Technology could change our lives*, EUR. PARLIAMENT (Feb. 2017), https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf (discussing changes in currencies, digital content, patents, e-voting, smart contracts, supply changes, decentralized autonomous organizations.).

announced the launch of a global carbon market for airlines based on blockchain technology.[75] AirCarbon will be the first multi-stakeholder carbon trading center in the world.[76]

However, some researchers have now casted doubt on the need for blockchain in industries where it supposed blockchain was most useful.[77] For example, in supply chain management, if employees are not trustworthy, a risk of compromising the whole supply chain exists. By contrast, if all employees are trusted, a blockchain is not needed. Therefore, from a macroeconomic perspective, prospects of establishing a single blockchain for every supply chain does not seem very efficient.

In the public sector, blockchain could play a significant role in relation to electoral processes. Open and fair electoral processes are a mainstay of democracy, and the immutability of blockchains makes them an excellent solution to ensure that votes are not being manipulated. However, imagine a system of e-voting enabled by a public blockchain technology that does not guarantee the maximum level of anonymity. In such a system, sophisticated entities such as governments and corporations could single out individuals according to political belief, compromising their fundamental right to data protection and privacy.[78]

In addition, it is noteworthy to mention that blockchain's advantages may not be considered necessary in other contexts, such as case management in international arbitration. Some reasons are related to the time and cost of processing blockchain-based transactions, the relatively common management of documents using third-party cloud storage providers by arbitral tribunals, and the fact that arbitral institutions already have in place a secured website.[79] This evidence suggests that not every problem in the digital space must be solved by blockchain technology, especially when the current system is efficient and trustworthy.

---

[75] @Operem, *Creating a Cleaner Future with AirCarbon*, MEDIUM (May 13, 2019), https://medium.com/@operem_corp/creating-a-cleaner-future-with-aircarbon-83b19243eccf.

[76] *Singapore-based AirCarbon Pte Ltd launches world's first digital aviation carbon exchange to fight climate change*, RHT FINTECH HOLDINGS PTE. LTD. (Oct. 30, 2019), https://www.rhtgoc.com/news/press-release/singapore-based-aircarbon-pte-ltd-launches-worlds-first-digital-aviation-carbon-exchange-to-fight-climate-change/.

[77] *See generally* Karl Wust & Arthur Gervais, *Do you Need a Blockchain?*, INT'L ASS'N FOR CRYPTOLOGIC RES. (2018), https://eprint.iacr.org/2017/375.pdf.

[78] *See* Guy Zyskind, Oz Nathan & Alex 'Sandy' Pentland, *Decentralizing Privacy: Using blockchain to Protect Personal Data,* 2015 IEEE CS SECURITY AND PRIVACY WORKSHOPS 180, 183 (2015) (discussing how certain anonymized datasets can be "de-anonymized" due to a "small amount of data points or high dimensionality data.").

[79] Ashish Chugh, *Why We Don't Need Blockchain to Manage Cases in International Arbitration*, KLUWER ARB. BLOG (May 13, 2018), http://arbitrationblog.kluwerarbitration.com/2018/05/13/dont-need-blockchain-manage-cases-international-arbitration/.

D. Limits of Blockchain

There is still a misconception around blockchain technologies (and cryptocurrencies) with regard to anonymity. Some claim that cryptocurrencies are by definition anonymous[80] or that blockchains ensure privacy thanks to a sophisticated asymmetric double key system, based on the use of two different keys.[81] Nonetheless, the degree of anonymity will depend on the underlying protocol in the blockchain. For example, transactions carried out by Bitcoin are not anonymous, as revealed in the Silk Road investigation.[82] A study classifies most cryptocurrencies as pseudo-anonymous[83] and, notably, the interference with privacy of individuals has motivated the creation of "altcoins."[84] Altcoins are all cryptocurrencies other than Bitcoin.[85] Privacy coins are an evolution of cryptocurrencies designed to ensure privacy for financial information of a user.[86] The coin can afford privacy of transactions by design (i.e. Monero or Zerocash)[87] or it can be an option for users (i.e. Zcash or Dash).[88] Therefore, it seems evident that in order to alleviate the privacy interference of a fully transparent blockchain, a number of techniques have been proposed. Creating privacy coins as alternative cryptocurrencies shows the awareness of users of their data protection rights.

One of the advantages of blockchain technologies is enhancing transparency and accountability of transactions. At least one study goes beyond this, claiming that "the popularity of blockchain technology may also

---

[80] *See* Nieves Pacheco Jiménez, *Criptodivisas: del Bitcoin al MUFG. El potencial de la tecnología Blockchain,* 19 REVISTA CESCO DE DERECHO DE CONSUMO 6, 7 (2016) ("son anónimas, permitiendo preservar la privacidad en las transacciones.").

[81] *See* JAVIER W. IBAÑEZ JIMÉNEZ, *DERECHO DE BLOCKCHAIN Y DE LA TECNOLOGÍA DE REGISTROS DISTRIBUIDOS* (Thomson Reuters Aranzadi, Cap. 1.I.7., 2018).

[82] *See generally* David Adler, *Silk Road: The Dark Side of Cryptocurrency*, FORDHAM J. OF CORP. & FIN. LAW (Feb. 21, 2018), https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/#_edn1.

[83] Dr. Robby Houben & Alexander Snyers, *Cryptocurrencies and blockchain*, EUR. PARLIAMENT 29 (July 2018), https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.

[84] *See* Mauro Conti et al., *A Survey on Security and Privacy Issues of Bitcoin*, CORNELL U. ARXIV tbl. V (Dec. 25, 2017), https://arxiv.org/pdf/1706.00916.pdf.

[85] Houben & Snyers, *supra* note 83, at 29.

[86] *See* Tiffany Madison, *Privacy Coins: How Monero, Dash, and ZCash Will Enable True Privacy*, MEDIUM (Mar. 28, 2019), https://blog.goodaudience.com/privacy-coins-what-you-need-to-know-975a3460d944; Conti et al., *supra* note 84, § 5.

[87] Zerocash is untraceable. ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 190 (drft. 2016), https://www.lopp.net/pdf/princeton_bitcoin_book.pdf. *See also* Aziz, *Guide on Privacy Coins: Comparison of Anonymous Cryptocurrencies*, MASTER THE CRYPTO, https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/ (last visited Mar. 24, 2020).

[88] Madison, *supra* note 86.

reflect an emergence social trend to prioritize transparency over anonymity."[89] However, in practice, natural and legal persons are not comfortable enough with the technology to publish all their information onto a public database,[90] in particular when sensitive information or financial information is at stake. The problem does not arise with legal persons because they do not have a right to personal data protection.[91] But, according to the Technology Director of the Open Data Institute, the transparency and irreversibility of blockchain technologies with regards to natural persons make them unsuitable for storing personal data.[92] This evidence suggests that blockchains cannot coexist with the GDPR.

Despite the advocates for blockchain technology, presently it is still a slower method for executing transactions. It takes ten minutes to mine each block,[93] which means that each transaction needs this period of time to become effective. Moreover, there is sometimes a waiting list, a "Mempool,"[94] as not all transactions can be packed in every block every ten minutes. So, it is not rare that the time may be extended during peak periods. For example, when comparing transaction speeds between credit cards and cryptocurrencies, in aggregate Visa and Mastercard can process, "more than 5,000 transactions per second with capacity to process volumes multiple times that number."[95] Visa can handle 1,700 transactions per second (tps) or around 150 million of transactions every day.[96] Meanwhile, Ethereum and Bitcoin only confirm 20 and 7 tps. respectively.[97] These numbers may be improved in the future, but it is argued that a potential limit for Bitcoin is 27

---

[89] Boucher et al., *supra* note 74, at 22.

[90] Vitalik Buterin, *Privacy on the Blockchain*, ETHEREUM BLOG (Jan. 15, 2016), https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain (mentioning the possibility that someone else related to a domestic or foreign government, business companies, coworkers and family members is able to see the information stored on a public blockchain).

[91] GDPR, *supra* note 10, ¶ 14.

[92] Umeh, *supra* note 52, at 61.

[93] *How Long Does It Take To Mine A Bitcoin?*, INVEST IN BLOCKCHAIN (Apr. 22, 2019), https://www.investinblockchain.com/how-long-does-it-take-to-mine-bitcoin/.

[94] Ofir Beigel, *The Bitcoin Mempool – A Beginner's Explanation*, 99 BITCOINS (Nov. 14, 2019), https://99bitcoins.com/bitcoin/mempool/.

[95] Ryan Vlastelica, *Why bitcoin won't displace Visa or Mastercard soon*, MARKETWATCH (Dec. 18, 2017, 8:24 AM), https://www.marketwatch.com/story/why-bitcoin-wont-displace-visa-or-mastercard-soon-2017-12-15.

[96] *See* Kenny Li, *The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed*, HACKERNOON (Jan. 26, 2019), https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44.

[97] *See* Sean Williams, *Which Cryptocurrencies Have the Fastest Transaction Speeds?*, THE MOTLEY FOOL (Jan. 14, 2018, 8:06 AM), https://www.fool.com/investing/2018/01/14/which-cryptocurrencies-have-the-fastest-transactio.aspx (discussing Ripple, a cryptocurrency that handles 1,500 tps.).

tps.[98] In general, it was pointed out that blockchain technologies are inefficient by design, because every fully potential node must proceed every transaction and maintain a copy of every state.[99] The qualities that benefit security come at the expense of performance. In a similar vein, blockchain technologies are considered not yet mature due to "severe technical and procedural limitations."[100] In brief, practical barriers prevent realizing a mainstream use of blockchain technologies.

Blockchain is presented as a solution for trustless environments. However, two premises follow. The first one is that users cannot do without trust in the system. The second one is that new intermediaries replace traditional intermediaries.

1. Users cannot do without trust in the system

Users cannot do without trust in the system, whether digital or analog. Blockchain does not move from a system where trust is necessary to another based on code where trust is unnecessary. The literature usually refers to a "trusted" record,[101] which suggests users begin to place confidence in the actors that make blockchain infrastructure possible. Without confidence in the developers or in the intermediaries that act as service providers, users would not use a blockchain system.[102] Another perspective to look at it is that users need to trust blockchain technology (the cryptography, the protocols, the software, the computers and the network). Bruce Schneier argues that there is no good reason to trust blockchain technology.[103] His

---

[98] Evangelos Georgiadis, *How many transactions per second can bitcoin really handle? Theoretically.*, INT'L ASS'N FOR CRYPTOLOGIC RES. (Apr. 1, 2019), https://eprint.iacr.org/2019/416.pdf.

[99] Preethi Kasireddy, *Fundamental Challenges with Public Blockchains*, MEDIUM (Dec. 10, 2017), https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428.

[100] MICHÈLE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE 31 (2018). *See generally* Edmund Schuster, *Cloud Crypto Land* (London Sch. of Econ. Law, Soc'y & Econ. Working Papers, Paper No. 17/2019, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3476678 ("Legal and practical obstacles therefore mean that, at least outside its original and circumscribed realm of cryptocurrencies, blockchain technology has no future.").

[101] *See, e.g.*, David Rountree, *Navigating the Blockchain and the Law*, 26 LSJ: LAW SOCIETY OF NSW JOURNAL 72 (2016).

[102] *See, e.g.*, Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries of the Public Blockchains*, *in* REGULATING BLOCKCHAIN. TECHNO-SOCIAL AND LEGAL CHALLENGES 58-81 (Hacker, P. et al eds., 2019); Rebecca M. Bratspies, *Cryptocurrency and the Myth of the Trustless Transaction*, 25 MICH. TECH. L. REV. 1, 18–46 (2018) (explaining the ledgers of trust embedded in cryptocurrencies in particular).

[103] Bruce Schneier, *There's No Good Reason to Trust Blockchain Technology*, WIRED (June 6, 2019), https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/ ("[Y]ou need to trust them absolutely, because they're often single points of failure . . . . Would you rather trust a human legal system or the details of some computer code you don't

arguments relate to the misplacement of trust from humans to technology as an abstract concept.[104] This demonstrates that trust in the system is still relevant.

In the context of cryptocurrencies, users need to rely on wallets[105] in order to complete transactions; or on exchanges[106] to carry out cryptocurrencies exchanges for fiat money.[107] Therefore, if someone pays with bitcoins, and sells bitcoins in exchange for a good, the individual will need a wallet of bitcoins or a wallet service in the cloud, where the bitcoins that are his/her "property" are stored. The privacy issue emerges while using the wallet. The individual needs a bitcoin address assigned by the intermediary and a user number, which can be traced to the origin of the transaction.[108] In some cases, even wallet services require users to register a phone number and an email address. This information allows the identification of the subject behind each transaction by combining the data of the Bitcoin address with the brokers' records, whether wallets or exchanges.[109] Users give up control of their bitcoins using an exchange or bitcoin wallet, because users do not generate their Bitcoin account and so they do not have their private key when signing with an intermediary (exchange or bitcoin wallet).[110] Rather, transactions are first authenticated between users and the trading venue. In spite of the initiative of users in generating a transaction, the final check is done by the exchange, so the exchange controls the transaction and sets limits.[111] In this scenario, users only order the intermediary to carry out certain transactions. As a result, users have no direct influence on data processing, but rather the intermediaries have a decisive influence on data processing.[112]

---

have the expertise to audit?").

[104] *Id.*

[105] Bitcoin wallets do not physically store the bitcoins, but instead store the public and private keys necessary to manage the bitcoins, which are on the network. NARAYANAN ET AL., *supra* note 87, at 112.

[106] An exchange is a service provider where suppliers and buyers of cryptocurrencies get in touch to exchange them for legal tender. *See, e.g.*, BITFINEX, https://www.bitfinex.com (last visited Mar. 26, 2020); POLONIEX, https://poloniex.com (last visited Mar. 26, 2020); KRAKEN, https//www.kraken.com (last visited Mar. 26, 2020). *See also* Becky Leighton, *What is a cryptocurrency exchange and how do they work?*, COIN INSIDER (Mar. 15, 2019), https://www.coininsider.com/cryptocurrency-exchanges/.

[107] *See generally* Bratspies, *supra* note 102.

[108] *See* Danny Bradbury, *How to Use Bitcoin*, THE BALANCE (Jan. 9, 2020), https://www.thebalance.com/how-to-use-bitcoins-391214.

[109] For example, see the Abra mobile Bitcoin wallet. Ofir Beigel, *Best Bitcoin Wallets for iOS (iPhone, iPad)*, 99 BITCOINS (Nov. 13, 2019), https://99bitcoins.com/bitcoin-wallet/ios-iphone-ipad/.

[110] Bacon et al., *supra* note 29, at 18–19.

[111] Jörn Erbguth & Joachim Fasching, *Wer ist Verantwortlicher einer Bitcoin-Transaktion?*, 12 ZEITSCHRIFT FÜR DATENSCHUTZ 560, 564 (2017)

[112] *Id.* at 565.

In addition, doubts about the reliability of companies supporting a cryptocurrency, like in the case of Facebook with Libra, confirms how a new cryptocurrency cannot stay without trust.[113] Facebook tries to build trust at least in two ways. First, working in collaboration with twenty-seven other companies and promising that the digital currency would be overseen by an independent nonprofit, called the Libra Association,[114] based in Switzerland.[115] Second, Facebook launched Calibra, which is its subsidiary that promises not to mingle users' Libra payments with Facebook data.[116] By contrast, the most famous cryptocurrency so far, Bitcoin, is successful because users trust it and think it has value.[117]

2. New intermediaries replace traditional intermediaries

One advantage of using blockchain is getting rid of third-party intermediaries, because algorithms would substitute the need of middlemen. Bitcoin, launched by the still-unknown Satoshi Nakamoto, was founded on a lack of trust, a problem that created and explained the financial crisis according.[118] The mere possibility of market reversal increases the need for trust. Therefore, an immutable record of ledgers can solve this issue in the future, since record-keeping will be public, decentralized, and tamper-proof. In addition, the intrinsic characteristics of the transactions' record will make intermediaries unnecessary. However, in the finance context, far from dispensing with the use of intermediaries, new intermediaries have arrived, benefiting from the legal framework gap surrounding cryptocurrencies.[119]

The promise that blockchain will make the middlemen disappear is reminiscent of the similarities of Amazon's first business model on the faith

---

[113] Roger McNamee, *We can't trust Facebook on elections, privacy or risks of a new Libra cryptocurrency*, USA TODAY (Oct. 24, 2019, 1:27 PM), https://www.usatoday.com/story/opinion/2019/10/24/dont-trust-facebook-elections-privacy-libra-terrible-idea-column/4075693002/.

[114] *See Joint statement on global privacy expectations of the Libra network*, INFO. COMMISSIONER'S OFF. (UK), https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf (last visited Jan. 26, 2020).

[115] *See Libra Association Pursues Payment System License Under FINMA Lead Supervision* (Sept. 11, 2019), https://libra.org/en-US/wp-content/uploads/sites/23/2019/09/Libra-Communiqué.pdf [hereinafter *Libra Association*].

[116] Josh Constine, *Facebook announces Libra cryptocurrency: All you need to know*, TECHCRUNCH (June 18, 2019, 5:01 AM), https://techcrunch.com/2019/06/18/facebook-libra/.

[117] *See* Larissa Lee, *New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market*, 12 U.C. HASTINGS BUS. L.J. 81, 89 (2016).

[118] Nakamoto, *supra* note 66, at 1.

[119] Timothy G. Massad, *It's Time to Strengthen the Regulation of Crypto-Assets*, (Harvard Univ., Working Paper No. 112, 2019), https://www.brookings.edu/wp-content/uploads/2019/03/Economis-Studies-Timothy-Massad-Cryptocurrency-Paper.pdf.

of "friction-free capitalism."[120] Selling directly to the consumer through the possibilities of the Internet would reduce the costs of intermediary services (warehouses, retailers, and distribution networks). Nevertheless, the location of a consumer is not irrelevant, because without a giant inventory and giant warehouses distributed throughout the world, Amazon could not meet the demand of consumers in the required time or deal with the inconveniences caused by returns.

The existence of cryptocurrencies proves that as new intermediaries (wallets, exchanges, oracles, etc.) emerge, the market for digital assets does not behave in the same way as the market of physical assets. For example, in Bitcoin's case, most users interact with blockchains through intermediaries.[121] Intermediaries will still need to manage changing circumstances, providing information, or connecting the blockchain data with other sources of data, such as national registries. Therefore, this supposedly miraculous technology engenders risks in terms of lack of regulation of activities, including intermediaries, at the expense of investor protection standards, often related to money laundering and cybercrimes.

III. THE EXTENSIVE TERRITORIAL SCOPE OF THE GDPR

A. Direct applicability throughout the European Union

The GDPR is directly applicable in all Member States.[122] It provides a uniform level of protection throughout the European Union, which overcomes some of the difficulties experienced by the application of national laws transposing the Data Protection Directive.[123] The Regulation has a two-fold purpose. The first purpose is to complete the legal gaps and ensure the effective exercise of the right to data protection, considering the fundamental right of data protection in article 8(1) of the EUCFR[124] and article 16(1) of the TFEU.[125] The second purpose is to ensure the free flow of personal data between Member States as part of the internal market.[126]

---

[120] "Friction-free capitalism" is a term coined by Bill Gates to refer the Internet as a powerful tool to eliminate the middleman in conducting transactions. *See* BILL GATES, NATHAN MYHRVOLD, AND PETER RINEARSON, THE ROAD AHEAD (1995).

[121] KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 98 (MIT Press, 2018).

[122] *See* GDPR, *supra* note 10, at art. 99.

[123] Data Protection Directive, *supra* note 23, art. 4.

[124] EUCFR, *supra* note 3, art. 8(1).

[125] TFEU, *supra* note 3, art. 16(1); GDPR, *supra* note 10, ¶1. *See* Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Protection Regulation*, in *New Technologies and EU Law*, *in* NEW TECHNOLOGIES AND EU LAW 151 (Cremona, M. ed., Oxford U. Press, 2017).

[126] *See* GDPR, *supra* note 10, ¶ 10.

The territorial scope of the GDPR determines under which conditions European law is applicable to activities carried out by controllers or processors of personal data, even though they may not be established within the European Union.[127] With a similar objective, the criteria for processing personal data is relevant to determine the competence of the supervisory authorities of Member States. A significant difference between the last regime and the current one is that the function of article 4 of the repealed Data Protection Directive[128] determined the national law applicable to a processing activity, meanwhile article 3 of the GDPR defines the territorial scope of the regulation. Nonetheless, it is worth mentioning that inasmuch as the GDPR leaves a margin of appreciation to Member States' national laws and that these laws are not uniform, it could be relevant to determine the applicable law of a Member State. In such a scenario, article 3 of the GDPR can be a useful source of inspiration to specify the national law applicable.[129] There are two alternative connecting factors that trigger the application of the GDPR: the establishment of a controller or processor within the European Union and the targeting and monitoring criteria for individuals located in the European Union.

B. Significance of establishment within the European Union

Pursuant to article 3(1) GDPR, the processing of personal data must be carried out in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in or outside the European Union.[130] This rule follows the Data Protection Directive criterion, where the location of a controller or a processor within the European Union is decisive.[131] Thus, regardless of the real location of the personal data processing, for example, in a third country where the parent company has its headquarters, when a corporation has a subsidiary in a Member State of the European Union, the GDPR may apply to the subsidiary.

In addition, GDPR refers to the establishment of the data processor and not only the controller, which is a novelty in comparison with the Data Protection Directive. This change expands the scope of the GDPR. A processor located in the European Union, that acts on behalf of a controller

---

[127] *Id.* art. 3.
[128] Data Protection Directive, *supra* note 23, art. 4.
[129] Pedro A. De Miguel Asensio, *Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea*, 69 REVISTA ESPAÑOLA DE DERECHO INTERNACIONAL (REDI) 75, 78 (2017).
[130] GDPR, *supra* note 10, art. 3(1).
[131] Data Protection Directive, *supra* note 23, art. 4.

outside the European Union, will have to respect E.U. law, which prevents the Union to become a data haven.

Moreover, a functional approach to determine an "establishment" prevails. According to GDPR recital 22, an "establishment" is understood as an effective and real exercise of activity through stable arrangements.[132] Therefore, the concept of an "establishment" is sufficiently flexible because "the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned."[133]

Yet, this interpretation does not mean that the concept of an "establishment" is defined without limits. The Court acknowledged in *Verein für Konsumenteninformation* that the mere fact of having an undertaking's website accessible in the European Union does not signify that a non-European entity has an establishment in the European Union.[134] Applying this ruling to a blockchain context, when validating nodes and participating nodes, that may be considered controllers or processors,[135] are established outside the European Union, the entity does not constitute an establishment in the Union merely due to the fact that the blockchain network is accessible in the Union. This situation often happens in a public and permissionless blockchain.

A more difficult notion to interpret is whether the activities of the controller or data processor related to personal data processing occurs "in the context of activities of" an E.U. establishment.[136] In the *Google Spain* case, the CJEU determined that a connection is necessary between the activities of the company carrying out the processing of data and the subsidiary established in the European Union.[137] Personal data processing occurs in the context of activities of an E.U. establishment when the activities of the controller situated in a third country are "inextricably linked" to the activities carried out by an establishment in a Member State.[138] For example, if the parent company is a social network in a third State, while the subsidiary, established in the European Union, sells food products without any

---

[132] GDPR, *supra* note 10, ¶ 22.

[133] Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, 2015 EUR-Lex CELEX 62014CJ0230, ¶ 29 (Oct. 1, 2015) [hereinafter Weltimmo].

[134] Case C-191/15, Verein für Konsumenteninformation v. Amazon EU Sàrl, 2016 EUR-Lex CELEX 62015CJ0191, ¶ 76 (July 28, 2016) [hereinafter Amazon EU Sarl].

[135] *See infra* Section V on the discussion about considering nodes controllers or processors.

[136] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 EUR-Lex CELEX 62012CJ0131, ¶ 55 (May 13, 2014) [hereinafter Google Spain].

[137] *See id.*

[138] *Id.* ¶¶ 55–56.

connection with the social network, there is no relationship in the context of the activities.[139] Conversely, the activities of the company situated in a third State and those of its establishment located in the Member State are "inextricably linked" when the activities serve to obtain funds that renders the activity of the company situated in a third State profitable.[140] *Google Spain* was a case that held a relationship exists between Google Inc. in the United States, and Google Spain SL in Spain, as the advertising space offered by Google Spain makes the search engine profitable.[141] Some criticism arose concerning the wide interpretation of processing of personal data "in the context of the activities" of an establishment of the controller in a Member State, because it could be used to cover situations with a lack of a significant link with the European Union.[142] However, on similar grounds, the CJEU recently confirmed that the activities of Google France related to the advertising space are inextricably linked to the processing of personal data carried out for the purposes of operating the search engine concerned.[143] Therefore, unsurprisingly, the activities of the establishment of Google France are covered by the scope of the Directive and the GDPR. Moreover, the processing of personal data is considered to be a single act due to the existence of gateways between its various national versions.[144]

> On the other hand, the European Data Protection Board advises that
> [T]he existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law.[145]

---

[139] Article 29 Data Protection Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, 176/16/EN WP 179 update, Annex 2 (Dec. 16, 2015).

[140] Google Spain, *supra* note 136, ¶ 55.

[141] *Id.* ¶ 56.

[142] See Lokke Moerel, *The long arm reach of EU data protection law: does the Data protection Directive apply to processing of personal data of EU citizens by websites worldwide?,* 1 INT'L DATA PRIVACY L. 28, 40–45 (2011); Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges*, *in* PROTECTING PRIVACY IN PRIVATE INTERNATIONAL AND PROCEDURAL LAW AND BY DATA PROTECTION 19, 28-31 (Burkhard Hess & Cristina M. Mariottini eds., 2015).

[143] Case C-507/17, Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des Libertés (CNIL), 2019 EUR-Lex CELEX 62017CJ0507, ¶ 52 (Sept. 24, 2019) [hereinafter Google LLC].

[144] *Id.*

[145] *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version adopted after public consultation*, EUR. DATA PROTECTION BOARD 7 (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_afte

It must be highlighted that regardless of the location or the nationality of the data subject whose personal data is being processed, when the processing occurs in context of the activities of an establishment of a controller or processor in the Union, it would fall under the scope of the GDPR.[146]

Locating a controller in a single jurisdiction is challenging in a public and permissionless blockchain. For example, Bitcoin has 1,803 nodes in Germany, 589 nodes in France and 468 nodes in the Netherlands, without prejudice of more nodes in other Member States.[147] As case law suggests, a broad interpretation of establishment of the controller would mean that where nodes, considered as controllers, exist in the European Union,[148] the GDPR applies to them. This view is problematic because it is impossible to determine the hierarchy of controllers for other nodes located in third countries. A possible indication would be to refer to the location of full nodes that keep all the ledger and, if they are located within the European Union, GDPR should apply. However, this solution would not solve the problem of a lack of reference to a "main establishment."[149]

By contrast, determining the establishment of the data controller would be easier if an identifiable person operates or established the blockchain, which is the case of a private and permissioned blockchain. For example, a consortium of banks or a financial entity that sets up a blockchain to manage clients' data.

C. The targeting and monitoring criteria to individuals located within the European Union

Regarding the first GDPR connecting factor, namely the establishment of controllers and processors in the European Union, companies without any establishment in the European Union, but those who process personal data of people in the European Union, would be exempted from complying with the GDPR. However, to avoid this problem, a second connecting factor exists (i.e. targeting and monitoring criteria for individuals located in the European Union). The GDPR shows an evolution in comparison with the rules set up in the repealed Directive. The Data Protection Directive focused on the equipment, automated or otherwise, for purposes of processing personal data by a controller not established in the European Union.[150] This approach was considered excessive and a source of legal uncertainty, because it could

---

r_public_consultation_en_1.pdf.

[146] *Id.* at 10.

[147] *Global Bitcoin Nodes Distribution*, BITNODES, https://bitnodes.earn.com (last visited Mar. 21, 2020).

[148] *See infra* Section V on the discussion about considering nodes controllers or processors.

[149] GDPR, *supra* note 10, ¶ 36.

[150] Data Protection Directive, *supra* note 23, art. 3.

cover situations that lacks a link with the European Union. For instance, this could apply to third country citizens who are not residents within the European Union.[151]

The new approach, which constitutes the second connecting factor, is based on a "targeting" criteria.[152] Under article 3(2) GDPR, when the controller or processor is located outside the European Union, the Regulation focuses on whether the processing activities are related to offering goods or services to data subjects situated in a Member State; or the processing activities relate to the monitoring of their behavior, as far as their behavior takes place in the European Union.[153] Interestingly, some versions of the GDPR refer to "residents" in the European Union, suggesting a protection limited only to residents in the European Union.[154] By contrast, other versions mention data subjects "who are" in the Union in conformity with GDPR recital 14, which covers "natural persons, whatever their nationality or place of residence."[155] The fact that GDPR was modified in comparison with the proposal of the Commission, at least in some versions, is in favor of the latter interpretation. The protection of personal data is enhanced with European rules, provided that natural persons (for example, users of blockchain) are in the European Union. Despite some language versions of the GDPR, it seems more appropriate to understand that the protection must be applied to natural persons, regardless of their nationality or place of

---

[151] De Miguel Asensio, *supra* note 129, at 80.

[152] *See* GDPR, *supra* note 10, ¶ 122.

[153] *Id.* art. 3(2) GDPR. *See* Hustinx, *supra* note 125, at 155.

[154] For references to "residents" under the GDPR, see art. 3(2) the Spanish version of the GDPR, in Reglamento (UE) 2016/679 Del Parliamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, 2016 O.J. (L 119) 1; and the Portuguese version of the GDPR, in Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), 2016 O.J. (L 119) 1.

[155] For references to data subjects "who are" in the European Union in accordance with recital 14 under the GDPR, see art. 3(2) the English version of the GDPR, in GDPR, *supra* note 10, at 1; the German version of the GDPR, in Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/45/EG (Datenshutz-Grundverordnung), 2016 O.J. (L 119) 1; the French version of the GDPR, in Règlement (UE) 2016/679 DU Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/45/CE (règlement general sur la protection des données), 2016 O.J. (L 119) 1; and the Italian version of the GDPR, in Regolamento (UE) 2016/679 Del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo ala protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), 2016 O.J. (L 119) 1.

residence.[156] The processing of users' personal data, to whom goods and services are directed, is the relevant element that determines that the obligations for processing of the controller(s) and processor(s) are governed by the GDPR. Therefore, the inclusion of clients or users residing in the European Union is an indication that the controller intends to offer goods and services to data subjects, whose personal data is processed, in the European Union.

Offering goods and services does not require a payment by the data subject. The difficult issue could be to establish when the controller or the processor plans to offer services to data subjects situated within the European Union. According to the jurisprudence from the CJEU, to determine the intention of a trader and a given consumer, certain types of information is not deemed sufficient evidence to indicate that a trader is directing its commercial activity to a Member State where the consumer has his habitual residence. A consumer contract is necessary in order to apply the rules of jurisdiction over consumer contracts, which contrasts with the rules on data protection, where no contract is pertinent. However, the list provided in the *Pammer* case can offer guidance for interpretation of the art. 3(2)(a) of the GDPR.[157] The *Pammer* criteria is not exhaustive; however, it can be useful to analyze if the controller or the processor envisages to offer services to data subjects situated in one or more Member States. For example, the trader's email or geographical address, or a telephone number without an international code do not indicate that a trader envisages conducting its activity in a Member State.[158]

On one hand, GDPR recital 23 states that the mere accessibility of the controller's, processor's, or the intermediary's website in the European Union, or the use of a language and a currency that is generally used in one or more Member States is not sufficient.[159] However, on the other hand, it is clear that the activities directed to one or more Member States when processing activities is related to the offering of goods or services, and effectively the consumer or user can order goods and services by selecting one language and one currency. Another pertinent factor is the inclusion of clients or users domiciled in the European Union. In addition, the use of a top-level domain name other than that of the Member State in which the controller or processor is established, or the use of neutral top-level domain

---

[156] EUR. DATA PROTECTION BOARD, *supra* note 145, at 15; De Miguel Asensio, *supra* note 129, at 85 (providing justifications for modifying the Commission proposal in the final Regulation.).

[157] De Miguel Asensio, *supra* note 129, at 84.

[158] *See* Joined Cases C-585/08 and C-144/09, Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG (C-585/08) & Hotel Alpenhof GesmbH v. Oliver Heller (C-144/09), 2010 E.C.R. I-12527 [hereinafter Pammer].

[159] GDPR, *supra* note 10, ¶ 23.

names such as ".com" or ".eu,"[160] represents further evidence that the controller envisages offering goods and services to data subjects in the Union. Thus, when it is apparent from the evidence, the controller or processor of data must comply with the GDPR.

For public and permissionless blockchains, it is likely that they fall under the application of the GDPR when there is an offer to use a service, such as bitcoin, thereby addressing data subjects in the European Union, despite the fact that anyone can register an account. Users do not maintain a contract with the software that allows the public blockchain infrastructure, so when users contract with the intermediaries (wallets and exchanges), they are required to be subject to the terms and conditions of the software. However, the terms and conditions of the platforms that support public and permissionless blockchains do not usually say anything about data protection.[161] For instance, it is not clear which is the legal basis to process data, according to the Bitcoin Core privacy policy, as there is not indication of any applicable law.[162] In contrast, Ethereum sets standard-form terms that cover data protection by reference to their privacy policy where they state to comply with the Swiss Federal Act on Data Protection ("FADP"), the Swiss Ordinance to the Federal Act on Data Protection ("OFADP") and the General European Data Protection Regulation ("GDPR").[163] According to their policy, Ethereum "contractually ensure that the protection of your personal data corresponds to that in Switzerland and the European Union at all times by concluding agreements using the standard contractual clauses and complying with the GDPR."[164] However, the fact that the terms of use of the website can change at the sole discretion of the Ethereum Foundation and are effective immediately could have a negative impact on users.[165] This situation contrasts with private and permissioned blockchain that could hamper Europeans to register on the platform and avoid being under the scope of the GDPR.

The last criterion to apply the GDPR is based on situations where Member State law applies by virtue of public international law (art. 3 (3) GDPR), even though a controller is not established in the Union.[166] This provision is not new, as it was already set in the Directive 95/46.[167] GDPR

---

[160] Pammer, *supra* note 158, ¶ 83.
[161] *See* Bacon et al., *supra* note 29, at 75.
[162] *See Privacy Policy*, BITCOIN, https://bitcoin.org/en/privacy (last updated July 5, 2016).
[163] *See Privacy Policy*, ETHEREUM, https://ethereum.org/privacy-policy/ (last updated Dec. 16, 2019).
[164] *Id.*
[165] See *Terms of use* ETHEREUM, (last uptodate Dec. 3, 2019) https://ethereum.org/terms-of-use/
[166] GDPR, *supra* note 10, art. 3(3).
[167] *Compare* Data Protection Directive, *supra* note 23, art. 4(1)(b).

recital 25 provides an example of a Member State's diplomatic mission or consular post.[168]

The extraterritorial scope of GDPR is sufficiently extensive to cover many blockchain platforms with regard to the location of nodes outside the European Union, provided that goods or services are offered to data subjects in the Union, or the processing activities are related to the monitoring of data subjects' behavior in the Union.

IV. DEALING WITH PERSONAL DATA IN BLOCKCHAIN

A. Identifiers: public keys and additional data

A first question that emerges with identifiers is which data used in relation to blockchain should be qualified as personal data. It must be stressed that data which potentially identifies a person is to be regarded as personal data.[169] Any objective or subjective information pertaining to the private life of a person is personal data.[170] GDPR recital 26 highlights a scenario where there is a reasonable likelihood that certain means are used to identify a natural personal, considering the available technology, the cost and the time required for identification.[171] According to Advocate General Campos Sánchez-Bordona, whose reasoning was followed by the CJEU in the *Breyer* case, the risk of identification appears to be insignificant if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of resources (such as time, cost and man-power).[172] Naturally, not only the data users, but also the data recipient may attempt to identify the individual, which must be taken into consideration. Definition of personal data could be surrounded by uncertainty, because data that apparently is not personal could become personal when technological developments are applied. Therefore, the possibility to infer information about natural persons from different kinds of data make it difficult to distinguish between personal and non-personal data.

On one hand, the GDPR provides a non-exhaustive list of identifiers: a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental,

---

[168] GDPR, *supra* note 10, ¶ 25.

[169] *See* GDPR, *supra* note 10, art. 4(1).

[170] Article 29 Data Protection Working Party, Opinion 04/2007 on the concept of personal data, at 6, 01248/07/EN WP 136 (June 20, 2007).

[171] GDPR, *supra* note 10, ¶ 26.

[172] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, Opinion of Advocate General Campos Sánchez-Bordona, 2016 EUR-Lex CELEX 62014CC0582, ¶ 68 (May 12, 2016) [hereinafter Breyer Advocate General Opinion].

economic, cultural or social identity of that natural person.[173] On the other hand, the CJEU has determined that an IP address is personal data.[174] Further examples of online identifiers are expressly mentioned in GDPR recital 30 such as cookie identifiers or radio frequency identification tags.[175]

Moreover, the identification of the data subject can be determined indirectly. The retained data may allow reaching very precise conclusions regarding the private lives of individuals, like "the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and social environment frequented by them."[176] For example, "dynamic" IP addresses may allow for indirect identification. "Dynamic" IP addresses are provisional addresses assigned for each internet connection and replaced when subsequent connections are made, as opposed to "static" IP addresses, which are invariable and allow continuous identification of the device connected to the network.[177] The CJEU held that dynamic IP addresses are personal data when the online media services provider has the legal means which may reasonably be used to identify the data subject, with the assistance of other persons, in particular the competent authority and the internet service provider, on the basis of the IP addresses stored.[178] The combination of information not necessarily in the hands of one person may enable the identification of the data subject.[179]

Consequently, there exists a broad meaning of personal data to cover any information that by reason of its content, purpose or effect, is linked to a particular person.[180] In light of GDPR recital 30, online identifiers are pseudonymous, but can become personal data "when combined with unique identifiers and other information receive by the servers, may be used to create profiles of the natural persons and identify them."[181] Bearing in mind that pseudonymous data qualifies as personal data,[182] the consequence is that public keys are personal data under the GDPR. Guidance from the Article 29

---

[173] GDPR, *supra* note 10, art. 4(1).

[174] Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2011 EUR-Lex CELEX 62010CJ0070, ¶ 51 (Nov. 24, 2011) [hereinafter Scarlet Extended]. This case relates to the situation in which the collection and identification of the IP addresses of Internet users is carried out by Internet Service Providers (ISPs).

[175] GDPR, *supra* note 10, ¶ 30.

[176] Digital Rights Ireland, *supra* note 8, ¶ 27.

[177] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, 2016 EUR-Lex CELEX 62014CJ0582, ¶ 16 (Oct. 19, 2016) [hereinafter Breyer CJEU Judgment].

[178] *Id*. ¶¶ 44–46, 48.

[179] *Id*. ¶ 43.

[180] Case C-434/16, Peter Nowak v. Data Protection Comm'r, 2017 EUR-Lex CELEX 62016CJ0434, ¶ 35 (Dec. 20, 2017).

[181] GDPR, *supra* note 10, ¶ 30.

[182] *See id.* art. 4(5).

Working Party broaches three criteria to determine the possibility of re-identification by: (1) singling out an individual; (2) linking records relating to an individual; and (3) inferring information concerning an individual.[183]

Public keys function as identifiers in a blockchain structure when they combine with other information. They can be considered a technology requirement to the functioning of the blockchain.[184] However, the option of using one-time public keys will minimize the risk of re-identification by singling out, linkability, or inference methods with additional data.[185]

Additional data are data related to the blockchain transaction. For example, assets exchanged, the qualifications of a person, address, financial data related to a natural person and any data that meets the requirement of identifying a person directly or indirectly. The French Data Protection authority recommends not to include additional data on a plain form and to use encryption techniques like commitment and keyed hash functions.[186]

B. Risks of re-identification

An aspect of uncertainty relates to what extent the data maintained in the blockchain ledger must be anonymized or deleted to comply with the principle of storage limitation, art. 5 (1) (e) GDPR.[187] The storage limitation principle means that the identification of data subjects cannot be for more than what is necessary for which the personal data is processed.[188] But not all techniques for anonymization are equally effective.[189] When the data subject is no longer identifiable because data has been anonymized, the respective data is no longer personal data. Therefore, this case is outside the scope of data protection law.

However, when data has been pseudonymized, they are still covered by the GDPR. According to E.U. law, "pseudonymisation" is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to

---

[183] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, at 3, 0829/14/EN WP 216 (Apr. 10, 2014) [hereinafter Anonymisation Techniques].

[184] *Blockchain: Solutions for a responsible use of the blockchain in the context of personal data*, COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS 7 (November 6, 2018), https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf [hereinafter CNIL].

[185] *See generally* Alex Biryukov et al., *Deanonymisation of clients in Bitcoin P2P network*, CORNELL U. ARXIV (July 5, 2014), https://arxiv.org/pdf/1405.7418.pdf (discussing a method to deanonymize Bitcoin users by linking public keys to IP addresses).

[186] CNIL, *supra* note 184, at 6.

[187] GDPR, *supra* note 10, art. 5(1)(e). The principle of storage limitation is also in the Modernized Convention 108. Convention 108, *supra* note 22, art. 5(4)(e).

[188] GDPR, *supra* note 10, art. 5(1)(e).

[189] *See generally* Anonymisation Techniques, *supra* note 183.

technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.[190] Data encryption can be the solution, as the pseudonym does not redirect to the data subject without knowing a decryption key. The issue of data encryption is that people not entitled to use the decryption key may still re-identify the data subject. The public key and transactional data on a distributed ledger can be deemed compatible with GDPR, only when they do not qualify as personal data. In contrast, when the public key and transactional data qualify as personal data, GDPR applies and compliance with the obligations by the controllers and processors is compulsory.

The Article 29 Working Party embraces a zero-risk approach, which means that the risk of identification after rendering data anonymous ought to be zero. Anonymization results from processing personal data in order to *irreversibly* prevent identification of the data subject.[191] However, some authors consider that a risk-based approach is compatible with GDPR recital 26.[192] This means that the question on the determination of personal data remains whether a reasonable risk of identification exists.[193] Only when the risk is negligible, data could be treated like anonymous data. It remains controversial if the GDPR imposes a zero-risk approach, considering that in line with recital 26, data becomes anonymous when "the data subject is not or no longer identifiable."[194] The problematic issue appears to be the inclusion of technological developments as an objective factor to identify a person. If assessing data is understood as a dynamic and periodical process, future re-identification of previously anonymized data could be a foreseeable scenario.[195]

Thus, establishing a high threshold like a zero risk of identification could not be realistic in the medium- and long-term for processing personal data through blockchains technologies. If a specific ledger is used for a specific time frame, it should be assessed for that period of time, considering that "[anonymization] should not be regarded as a one-off exercise and the attending risks should be reassessed regularly by data controllers."[196] Nevertheless, the fact that a ledger is seen as an immutable record of transactions without a specific time frame envisages that most data could at some point make identifiability possible, either by singling out an individual, linking records or making inferences from the information available. If we

---

[190] GDPR, *supra* note 10, art. 4(5).

[191] Anonymisation Techniques, *supra* note 183, at 6.

[192] GDPR, *supra* note 10, ¶ 26.

[193] Finck, *supra* note 27, at 19.

[194] GDPR, *supra* note 10, ¶ 26.

[195] *See* Anonymisation Techniques, *supra* note 183, at 15.

[196] *Id.* at 4.

assume that anonymization or personalization is not an isolated property of data but a property of the environment of data,[197] one practical solution could be to consider payload added to the blockchain as personal data, when designed to be used without a time limitation,[198] because it would be foreseeable that the desired identification would be possible in the future.

Another important aspect to consider is from which perspective the likelihood of identifying natural persons should be examined. It seems appropriate that only the data controller should be considered. The opening view of analyzing the possibility of identification from a third party may be burdensome. For example, initiating legal proceedings against a third person who has the additional information to make possible the identification of the data subject does not seem a reasonable option. For these purposes, the CJEU in the *Breyer* case notices that "it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored."[199] In this sense, the means may be understood as political or legal power of a State. In *Breyer*, even though the judgment refers to the State acting as an individual, the CJEU considers that legal channels exist for the German Federal institutions, who provide the online media services and who are responsible for the processing of dynamic IP addresses in the event of cyberattacks.[200] So, the online media services provider is able to contact the competent authority, who can take the steps necessary to obtain information from the internet service provider and bring criminal proceedings.[201]

However, an individual (not a State) does not usually have the necessary means unless he or she is the data controller or the data processor of the data. Imagine a user in a blockchain must resort to initiate legal proceedings against a third person who has the additional information to make possible the identification of the data subject. Under this scenario, it does not seem reasonably likely that he or she can access the personal information.[202]

---

[197] Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data - False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, 34 WIS. INT'L L.J. 284, 311–312 (2016).

[198] Finck, *supra* note 27, at 24.

[199] Breyer CJEU Judgment, *supra* note 177, ¶ 48.

[200] *Id.* ¶ 47

[201] *Id.*

[202] *See* Gerald Spindler & Philipp Schmechel, *Personal Data and Encryption in the European General Data Protection Regulation*, 7 J. OF INTELL. PROP., INFO. TECH. AND E-COMMERCE L. 163, 173 (2016) (discussing encrypted data as anonymous information).

V. ALLOCATION OF RESPONSIBILITY TO PARTICIPANTS

The distribution of responsibility for blockchain functions is a thorny issue. Lack of legal certainty and lack of agreement on interpretation between the supervisory authorities in the European Union is creating a sense of de-regulation of blockchain technologies. However, determining who is a "data controller" or a "data processor" becomes essential in order to exercise responsibilities that come into force and data subjects can claim and exercise their fundamental rights established in article 8 of the EUCFR and reinforced by the GDPR.

A. Data Controller

The importance of identifying a data controller is two-fold. First, it defines the degree of responsibility for participants, consequently, the scope of accountability and the degree of eventual liability. Second, it enables communications from data subjects and data protection authorities to data controllers. A specific contact may be necessary for data subjects in order to exercise their rights, such as the right to an effective judicial remedy against a controller or processor enshrined in article 79 of the GDPR.[203] Likewise, an identified data controller ensures supervisory authorities to be able to exert its investigative and corrective powers under article 58 of the GDPR, which includes to notify controllers or processors of an alleged infringement or any other contact necessary to carry out its tasks.[204]

The underlying assumption of reckoning with a data controller in any case of processing of personal data may be challenged by blockchain's functioning. The usual infrastructure is decentralized and connected but independent. Different players compose the network without an apparent hierarchy among them. In a public and permissionless scenario, it may be particularly burdensome to distribute responsibility among the players. Yet, allocating responsibility is essential to allow data subjects make complaints against controllers. At the same time, controllers have a wide range of tasks and bear the burden of proof of compliance with data protection rules and principles laid down in article 5(1) of the GDPR.[205]

Under E.U. law, a controller is defined as a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of the data.[206] Thus, where the person decides why and how data shall be processed he or she is deemed to be a controller. Convention 108 defined it in a different way,

---

[203] GDPR, *supra* note 10, art. 79.
[204] *See id.* art. 58.
[205] *Id.* art. 5(1).
[206] *See id.* art. 4(7).

giving examples of what you need to "control" to be considered a controller.[207] For instance, who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored, and which operations should be applied to them are considerations for establishing a controller.[208] Therefore, the traditional concept of controller under the Council of Europe Convention played a limited role in comparison with a dynamic and wider scope of "controller" under E.U. law.

First, the notion of "controller" is built independently and autonomously from national laws in contrast to the legal conferral necessary under Convention 108. Second, according to the Article 29 Working Party, the concept of "controller" is functional based on a factual analysis.[209] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) case illustrates the importance of a factual analysis. SWIFT is a company offering standardized messaging services to financial institutions. Its structure is a cooperative network with their headquarters in Belgium, operating centers in Europe and the United States, and branches in several E.U. Member States.[210] While SWIFT was formally considered a processor of personal data in messages between financial institutions, it *de facto* acted as a data controller, at least to the extent when it decided to transfer financial personal data to U.S. authorities through a non-transparent agreement without informing the financial institutions concerned.[211] Pursuant to Article 29 Working Party, a significant degree of autonomy and an effective margin of maneuver were decisive in considering SWIFT a controller.[212] Besides, processing personal data for the purpose of fighting against terrorism was incompatible with the original commercial purpose for which personal data has been collected.[213] Therefore, the identification of a controller in terms of conditions or a legal contract is not final, as long as it can be modified by a court judgement under a functional approach, rather than a formal analysis. Reflections on the different type of players in a public and permissionless blockchain are considered below.

---

[207] *See generally* Convention 108, *supra* note 22.
[208] *Id.*
[209] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", at 1, 00264/10/EN WP 169 (Feb. 16, 2010) [hereinafter Concepts of "Controller" and "Processor"].
[210] Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), at 9, 01935/06/EN WP 128 (Nov. 22, 2006) [hereinafter SWIFT Personal Data Processing].
[211] *Id.* at 11.
[212] *See id.*
[213] *Id.* at 15.

1. Developers

Developers do not process personal data, unless they run nodes or mine new blocks. However, developers of the code control the core software, which potentially give them a high degree of control over how processing data (eg. Bitcoin). Yet, even with the option to design, developers may not qualify as controllers, because they only make available the software to the user. Indeed, they neither have control over the use of the software nor on which content is actually stored on it.[214] They determine neither the concrete purposes nor the means of data processing. This perspective from a micro-level can be convincing, but from a macroeconomic level, developers have a function in why and how a blockchain is structured. They can design default blockchains that comply with GDPR when it is agreed that personal data are processed on a specific blockchain.

Preventing any liability of developers excluding them from being controllers might not seem reasonable in comparison to users; for the mere fact that users of a blockchain are controllers but they do not have any real alternative to use another type of blockchain for a specific transaction, for example, exchanging bitcoins.[215] The use of blockchains to offer services to E.U. citizens or residents is enough to trigger the territorial scope of application of the GDPR.[216] In order to comply with GDPR, developers that plan to create a public blockchain to exchange real estate, should comply with privacy by design and by default.[217] This means that they should be encouraged to creating blockchain solutions with privacy as an initial consideration rather than as an add-on "when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data."[218] Indeed, developers should design a system "with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."[219] Some suggest that blockchain developers will in many cases be forced to contend with "partial solutions, heuristics and mechanisms that are designed to bring privacy to specific classes of applications."[220] But is it

---

[214] Erbguth & Fasching, *supra* note 111, at 564.

[215] See *infra* § V.A.3.

[216] See *supra* § III.

[217] *See, e.g.*, Christian Wirth & Michael Kolain, *Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data*, *in* PROC. OF THE 1ST ERCIM BLOCKCHAIN WORKSHOP 2018, REP. OF THE EUR. SOC'Y FOR SOCIALLY EMBEDDED TECH. 5 (Wolfgang Prinz & Peter Hoschka eds., 2018), *available at* https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf

[218] GDPR, *supra* note 10, ¶ 78.

[219] *Id.*

[220] Buterin, *supra* note 90.

not the essence of Article 8 of the EUCFR to adopt "technical and organizational measures" which are able to ensure that personal data is given effective protection against any risk of abuse and against unlawful access and use?[221]

A projection of the reasoning of the Working Party on the determination of who are controllers for data processing in social networks to the context of blockchain can clarify the issue of controllership. In principle, the entity that offers the blockchain can be deemed to establish the "means for processing the user data" and consequently, that entity will be responsible for the "means" being developed following the privacy-by-design requirements. Therefore, it seems unlikely that public blockchains that do not have a governance mechanism will be accepted by regulators, particularly when consumer rights are at stake.[222]

2. Miners and Nodes

Miners run the protocol and play a leading role for the operation of a blockchain infrastructure because they gather transactions in new blocks according to a consensus mechanism, such as proof-of-work.[223] Nodes add data to the shared ledger and store a copy of the ledger in the devices.[224] They maintain the infrastructure in exchange of a reward, usually a cryptocurrency; but miners do not control the content of the data transfer.[225]

On one hand, without the work of miners, blockchains may not function. Thus, miners are responsible for the means. However, they do not define the purposes of a transaction because they act on behalf of users.[226] For the latter reason miners may not be considered "controllers." Some authors have advanced that the role of nodes and miners in Bitcoin is passive as they merely process the bitcoin sender and recipient's addresses, the public key of the transaction sender, the public key of the transaction recipient, a cryptographic hash of the transaction content, the amount of BTC,

---

[221] Digital Rights Ireland, *supra* note 8, ¶¶ 40, 66-67; Finck, *supra* note 27, at 85.

[222] Lokke Moerel, *Blockchain & Data Protection ... and Why They are not on a Collision Course*, 26 EUR. REV. OF PRIV. L. 825, 844 (2019).

[223] Other consensus mechanisms exist, such as Proof of Stake (PoS), Practical Byzantine fault tolerance (PBFT), Delegated Proof of Stake (DPoS) and Scalable Byzantine Consensus Protocol (SCP) Design. Joshi et al., *supra* note 41.

[224] Shaan Ray, *The Difference Between Blockchains & Distributed Ledger Technology*, TOWARDS DATA SCIENCE (Feb. 19, 2018), https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92.

[225] Mario Martini & Quirin Weinzierl, *Die Blockchain-Technologie und das Recht auf Vergessenwerden*, 36 NEUE ZEITSCHRIFT FÜR VERWALTUNGSRECHT 1251, 1253 (2017), *available at* https://www.uni-speyer.de/fileadmin/Lehrstuehle/Martini/BlockchainundRechtaufVergessenwerdenTyposkriptversion20-03-19NZ.pdf.

[226] Finck, *supra* note 27, at 46.

and the date and time of the transaction.[227] Miners, neither alone nor jointly, have influence on the inclusion of the transactions in the Bitcoin blockchain.[228] If a single miner places an invalid transaction in his block, his block will be discarded by the remaining miners. Miners have the opportunity to exclude certain transactions, but the group of miners cannot be clearly determined either, unless it is a mining pool. For reasons of security rather than privacy, a pool of more than 50% of Bitcoin's total computing power endangers the confidence in Bitcoin, so mining pools themselves ensure that they remain below the 50% limit.[229] As a result, nodes and miners in Bitcoin do not decide on the purpose and the means of data processing, so they should not be considered controllers.[230]

On the other hand, nodes can have different functions, but usually initiate a transaction or save a copy of the transaction in its database. First, to determine controllership "in case of doubt, other elements than the terms of a contract may be useful to find the controller, such as the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility."[231] According to some authors, miners pursue its own interest whilst registering and verifying whether transactions have the format or signatures, apart from storing data.[232] They maintain the ultimate authority to adopt a new software which modifies or amends a blockchain protocol.[233] Besides, "miners can rewrite the transaction history of the shared database or implement additional controls that shape how information is stored, processed, and recorded."[234]

It has been pinpointed that in practice, treating miners as controllers will not be feasible in large public blockchains, considering the case of proof-of-work consensus.[235] However, the relative importance of a node does not come from its special characteristics, but from its ability to contribute to the effectiveness of the network to achieve its objectives, defined by the

---

[227] *See* Bacon et al., *supra* note 29, at 69–70.

[228] Merlinda Andoni et al., *Blockchain technology in the energy sector: A systematic review of challenges and opportunities*, 100 RENEWABLE & SUSTAINABLE ENERGY REVS. 143, 149 (2019), *available at* https://reader.elsevier.com/reader/sd/pii/S1364032118307184?token=B0FB7362162E9FB3BECBD0091A07667E2F8F6A85AC1AFF34FF1695688345C3906165B3364D92618942E94DA49E643DC2.

[229] Erbguth & Fasching, *supra* note 111, at 564.

[230] *Id.* at 563–64.

[231] Concepts of "Controller" and "Processor", *supra* note 209, at 12.

[232] Martini & Weinzierl, *supra* note 225, at 1253.

[233] DE FILIPPI & WRIGHT, *supra* note 36, at 180.

[234] *Id.*

[235] Jacek Czarnecki, *Blockchains and Personal Data Protection Regulations Explained*, COINDESK (Apr. 26, 2017), https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained.

values and interests programmed in the networks.[236] Along the same lines, if it is not feasible to consider miners as controllers, the same conclusion could be reached in relation to nodes as controllers.

Nevertheless, recent literature shows that qualifying nodes as controllers is an option, when they verify the format of the transactions, participate in the validation of new blocks, or store a copy of the blockchain.[237] Besides, miners have the ability to discern whether a transaction is cryptographically or technically valid.[238] Consequently, they can be considered controllers because they participate in the network for their own benefit.

For example, the Libra Association, established in Switzerland,[239] would be considered a controller if processes personal data with a significant level of autonomy in relation to the cryptocurrency libra. The reasoning is similar to the SWIFT case, where the level of autonomy in deciding to establish a data hub in the United States and disclosing of data to U.S. authorities were decisive in assessing that SWIFT was a controller in relation to its personal data processes.[240]

In cloud contexts, providers of cloud computing services are processors when they offer computer resources to store data. It is considered that the cloud provider is merely processing personal data on behalf of the customer who is the controller. A processor means "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[241] Following this reasoning, nodes and miners are likely to be considered processors when they facilitate users to store and transfer information, as the users submit the personal data for their own purpose. This approach is shared with CNIL. Miners can be processors and not controllers because they are only validating transactions, rather than defining the purposes and means of the processing.[242]

Overall, the relevant aspect is whether nodes and miners are processing personal data on behalf of users or whether they are taking an active role. If they adopt a passive role facilitating the transactions, they still should be regarded as processors by analogy with cloud providers.

---

[236] MANUEL CASTELLS, COMUNICACIÓN Y PODER 45 (2009).

[237] *See generally* Thomas Buocz et al., *Bitcoin and the GDPR: Allocating Responsibility in distributed networks*, 35 COMPUTER L. & SECURITY REV. 182 (2019); Martini & Weinzierl, *supra* note 225, at 1253.

[238] DE FILIPPI & WRIGHT, *supra* note 36, at 181 ("miners may lack the capability to identify lawful or unlawful transactions flowing through a blockchain-based network.").

[239] *See Libra Association*, *supra* note 115.

[240] SWIFT Personal Data Processing, *supra* note 210, at 11.

[241] GDPR, *supra* note 10, art. 4(8).

[242] *See* CNIL, *supra* note 184, at 4.

3. Users

Part of the literature suggests that users are controllers with relation to their own data and the others' personal data.[243] At first sight, this consideration appears to be affirmative. The decision of users to utilize a blockchain network triggers the applicability of a data controller's obligations. In bitcoin's case, the sender and recipient's Bitcoin addresses and transactional data are personal data. Therefore, a user who decides to send an amount of Bitcoins to a recipient determines the purpose (transferring ownership over a token) and the means of processing. From this perspective, nodes and miners are acting on behalf of users. The CJEU emphasized that the definition of the concept of "controller" deserves a broader interpretation in order to ensure an effective and complete protection of data subjects.[244] In *Google Spain*, the fact that a search engine does not exercise control over the personal data published on the web pages of third parties does not lead to an exclusion of controllership by the operator of the Google search engine.[245] Therefore, users are the only data controllers, disregarding of the level of control on the personal data.

However, the problem of applying this approach to blockchain networks is the current imbalance between individual users and large service providers, such as mining pools. An application of an analogy of the cloud environment does not seem appropriate, because that demands users choosing blockchain networks that comply with data protection regulation.[246] Some type of guidelines from networks or from third parties that certify whether a blockchain network abide by privacy laws are necessary to take an informed decision about the blockchain technologies that are compliant with data protection laws. Without any kind of advice, determining whether a blockchain network is GDPR-compliant seems tricky. Would it be reasonable for a mere notice appearing in the network stating that a specific blockchain network is compliant with GDPR? Appropriate awareness from the outset is essential to make an informed choice as a customer-user.

The certification mechanism pursuant to article 42 of the GDPR could be useful for the purpose of enhancing transparency about the embedded software of a specific blockchain technology.[247] Although this certification is not mandatory, its voluntary character[248] would be a good step in the

---

[243] *See* Bacon et al., *supra* note 29, at 69–70.
[244] Google Spain, *supra* note 136, ¶ 30.
[245] *Id.* ¶ 34.
[246] *See* Bacon et al., *supra* note 29, at 69–79.
[247] *See* GDPR, *supra* note 10, art. 42.
[248] *Id.* art. 42(3).

direction of facilitating users to take an informed decision about choosing an application that is GDPR-compliant.

4. Household exemption for users

When a person enters personal data on a blockchain, the key question to answer is whether the individual acts in relation to a household activity or to a commercial or professional activity. In the first scenario, a person who only buys and sells bitcoins on his behalf cannot be considered a data controller. In contrast, if the same activity is carried out by the same person, but on behalf of another natural person, he or she can be deemed to be a data controller.[249] It can entail that the data controller does not necessarily own the data.[250] However, the guidelines from CNIL are not in line with the strict interpretation of the household exemption developed by the CJEU case law.

First, in the *Bodil Lindqvist* case, the criteria is not only the nature of the activity (private versus commercial), but also the scope of the dissemination of personal data.[251] The uploading of personal data on a website, making it accessible to an indefinite number of people changes the situation. Consequently, the shield of the household exemption disappears. The possibility to monitor blockchain transactions recorded on a public and permissionless blockchain allows anyone to see personal data, even without downloading the software.[252]

Regarding the scope of dissemination, the guidelines offered by the Article 29 Working Party on online social networking can be useful. The Social Networking Service (SNS) providers and third-party application providers are data controllers, but users can also be considered data controllers.[253] The difficult task is to determine when a user is acting out of the household exemption, so duties and responsibilities with data protection applies. The configuration of a user profile as public, for example, which permits anyone on the social network to see postings from the user or having data indexed by search engines available to a high number of contacts are indications that access goes beyond self-selected contacts, and therefore, beyond private and family life of the individuals.[254] The CJEU has

---

[249] CNIL, *supra* note 184, at 1–2.

[250] Some have also defined the data controller as someone who collects their own data. STEFAN LOESCH, A GUIDE TO FINANCIAL REGULATION FOR FINTECH ENTREPRENEURS 187-194 (2018).

[251] Case C-101/01, Criminal proceedings against Bodil Lindqvist, 2003 E.C.R. I-12971, ¶ 47 (Nov. 6, 2003) [hereinafter Bodil Lindqvist].

[252] *See* BLOCKEXPLORER, *supra* note 67.

[253] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, at 3, 01189/09/EN WP 163 (June 12, 2009) [hereinafter Online Social Networking].

[254] *Id.* at 6.

reaffirmed a restrictive approach to the household exemption in three cases: *Satamedia*,[255] *Rynes*,[256] and *Sergejs Buivids*.[257]

In *Rynes*, the fact that the camera recording was installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but that it also monitored part of the public space and was stored on a continuous recording device made the CJEU exclude such processing of data from the course of a purely personal or household activity.[258]

The *Sergejs Buivids* case concerned a citizen who published a video on YouTube recorded on a police station while he was making a statement in the context of administrative proceedings which had been brought against him. The citizen did not inform the police officers of the intended purpose of the processing of personal data concerning them. He posted on YouTube without restricting access to that video, thereby permitting access to personal data to an indefinite number of people. The court concluded that the processing of personal data at issue in the main proceedings did not come within the context of purely personal or household activities.[259]

It should be kept in mind that, when the household exception is inapplicable, the user may benefit from other exemptions and derogations, such as journalistic, artistic or literary purposes.[260] In these cases, a balance must be struck between privacy and freedom of expression. However, exemptions and derogations to the protection of the fundamental right to data protection must apply only in so far as it is strictly necessary.[261] Processing personal data that has been available in the media does not imply to be

---

[255] *See* Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy & Satamedia Oy, 2008 E.C.R. I-09831 (Dec. 16, 2008) [hereinafter Satamedia].

[256] *See* Case C-212/13, František Ryneš v. Úrad pro ochranu osobních údaju, 2014 EUR-Lex CELEX 62013CJ0212 (Dec. 11, 2014) [hereinafter Rynes].

[257] *See* Case C-345/17, Proceedings brought by Sergejs Buivids, 2019 EUR-Lex CELEX 62017CJ0345 (Feb. 14, 2019) [hereinafter Sergejs Buivids].

[258] Rynes, *supra* note 256, ¶¶ 30–33. "[W]here the activity in the course of which that processing is carried out is a 'purely' personal or household activity, that is to say, not simply a personal or household activity." *Id.* ¶ 30.

[259] Sergejs Buivids, *supra* note 257, ¶ 43. With regards to the balance between privacy and the freedom of information, the CJEU relies on the criteria established by the judgment of ECtHR in *Satamedia* where, *inter alia*, the contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and the manner and circumstances in which the information was obtained and its veracity. Satamedia, *supra* note 255, ¶ 66.

[260] *See* GDPR, *supra* note 10, art. 85.

[261] Satamedia, *supra* note 255, ¶ 56. Note that the CJEU only refers to the right to privacy, however, the issue in this case involves the fundamental right to data protection, as the Data Protection Directive applies.

outside the scope of data protection rules.[262] The CJEU held that if the activities' object of a company is solely the disclosure to the public of information, opinions or ideas, irrespective of the medium used to transmit processed data, the activities can benefit from the journalist exception.[263] The exception is not only available to media undertakings and can be used for profit-making purposes. The *Satamedia* case involved collection of fiscal data published in public documents related to income taxes and wealth taxes and then, published it on a newspaper, with the identification of the municipality and surname of individuals, transferred onward on CD-ROM to be used for commercial purposes and making it available by a text-message service surname. The CJEU left to national courts to decide if the private company, Satamedia, could be covered by the exemption of journalistic purposes. Finnish authorities considered that publishing of taxation information to such an extent shall not be regarded as journalism, but as processing of personal data which a company had no right to do.[264]

This ruling has been confirmed by the ECtHR, which accepts the ruling by the Finnish authorities, as the derogation for journalistic purpose in article 9 of the Data Protection Directive must be subject to strict interpretation.[265] According to the ECtHR, "the existence of a public interest in providing access to, and allowing the collection of, large amounts of taxation data did not necessarily or automatically mean that there was also a public interest in disseminating en masse such raw data in unaltered form without any analytical input."[266] It has been interpreted that the concept of "journalism" suffers from a reduction, in contrast to recital 153 and article 85 of the GDPR, which embrace a broader concept of freedom of expression and information.[267]

---

[262] Google Spain, *supra* note 136, ¶ 30.

[263] Satamedia, *supra* note 255, ¶ 61.

[264] *See id.*

[265] *See* Satakunnan Markkinapörssi Oy & Satamedia Oy v. Finland, App. No. 931/13, HUDOC EUR. CT. H.R. 1 (June 27, 2017), http://hudoc.echr.coe.int/eng?i=001-175121 [hereinafter Satamedia Grand Chamber]. Before this ruling, the Fourth Section Chamber of the European Court of Human Rights held that there was no violation of the right of freedom of expression under article 10 of the ECHR. *See* Satakunnan Markkinapörssi Oy & Satamedia Oy v. Finland, App. No. 931/13, HUDOC Eur. Ct. H.R. ¶ 50 (July 21, 2015), http://hudoc.echr.coe.int/eng?i=001-156272 [hereinafter Satamedia Fourth Section Chamber]. However, Judge Tsotsoria's dissenting opinion is relevant. *Id.* at 29. She considers the fact that personal data that has already been in the public domain to be very significant. *See id.* Ultimately, the Grand Chamber ruled that there was no violation of article 10 of the ECHR by a 15-2 vote, with remarkable dissenting opinions by Judges Sajó and Karakas. *See* Satamedia Grand Chamber, *supra* at 64.

[266] Satamedia Grand Chamber, *supra* note 265, ¶ 175.

[267] Dirk Voorhoof, *No journalism exception for massive exposure of personal taxation data,* STRASBOURG OBSERVERS (July 5, 2017), https://strasbourgobservers.com/2017/07/05/no-journalism-exception-for-massive-exposure-of-personal-taxation-data/#more-3801

B. Joint Controllership

Several participants acting as a group can share its responsibility. Under article 26 of the GDPR,[268] all participants in a public and permissionless blockchain can be deemed joint controllers, but they will need to distribute responsibilities. The CNIL recommends to select one participant as a data controller where that participant makes decision for the group.[269] This situation would avoid joint controllers, but absent the identification of a data controller, potentially all participants can be considered data controllers, subject to GDPR article 26 with the subsequent shared responsibilities.

Advocate General Jääskinen warned against the risks of broad definitions of personal data, processing of personal data and controller, because they "are likely to cover an unprecedently wide range of new factual situations due to technological development."[270] In his opinion, the CJEU should apply the principle of proportionality, a rule of reason, in interpreting the scope of the Data Protection Directive in order to avoid unreasonable and excessive legal consequences.[271] By the same token, the CJEU decided in *Bodil Lindqvist* regarding the transfer of personal data to third countries in the context of the Internet.[272] It rejected a wide scope of application of article 25 of the Data Protection Directive. Therefore, a moderate approach can avoid the unreasonably wide scope of application of the GDPR to define joint controllership for public blockchains.

However, the CJEU has confirmed a broad interpretation of the concept of joint-controllership in the *Wirtschaftsakademie Schleswig-Holstein* case.[273] The administrator of a fan page hosted on Facebook must be categorized as a joint-controller, together with Facebook. The administrator may define the parameters of the target audience and the objectives of managing and promoting its activities, contributing to the processing of the personal data of visitors to its page. It was decisive that the administrator of the fan page can ask for demographic data, location data and consumer behavior on line related to the target audience. Moreover, the administrator of a fan page was contributing to install cookies on devices of visitors since the moment they visit the mentioned fan page, whether or not the visitor has a Facebook account. The CJEU held that the joint

---

[268] GDPR, *supra* note 10, art. 26.

[269] CNIL, *supra* note 184, § 3.

[270] Google Spain, *supra* note 136, ¶ 30.

[271] *Id.*

[272] *See generally* Bodil Lindqvist, *supra* note 251.

[273] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, 2018 EUR-Lex CELEX 62016CJ0210 (June 5, 2018) [hereinafter Wirtschaftsakademie].

responsibility is shared between the operator of the social network and the administrator of a fan page hosted on that network, which is justified to ensure more complete protection of the rights of persons visiting a fan page concerning the processing of their personal data.[274] Thus, the concept of data controller deals with assigning responsibilities based on the ability to influence the purpose and method of data processing, which inevitably results in a case-by-case analysis. Yet, it must be emphasized that joint controllership neither imply equal responsibility of the various operators involved in the processing of personal data nor it is required each of the co-responsible to have access to the personal data concerned.[275]

Further, the *Fashion ID* case advocates for a wide interpretation of joint-controllership.[276] The case was related to the Facebook "like" plugin that is embedded on a web page (Fashion ID). The operator of a web page becomes responsible for the processing of personal data by the mere fact of inserting a plugin, and regardless of whether the administrator of a website does not have the ability to determine the data that the browser transmits or what the external provider does with the data. That is, despite not having control over whether the external provider (Facebook) decides to store or to analyze the data, the operator of that website is responsible for the operations of collecting and transmitting personal data of its visitors. Particularly relevant is the fact, that the CJEU considers that Fashion ID has consented, "at least implicitly, to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage consisting in increased publicity for its goods."[277]

According to the CJEU, two reasons are significant in order to reach the conclusion that Fashion ID is a controller. First, it appears to be the awareness of the administrator of the website. Fashion ID has exerted a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin by embedding that social plugin on its website.[278] Therefore, without that plugin the collection and transmission of personal data of visitors to that website would not have occurred. Second, the Court distinguishes that the responsibility of the operator of a website is greater vis-à-vis those who are not members of Facebook in comparison with those who are members of the social network. With regard to those not members of the social network, in a similar way to

---

[274] *Id.* ¶ 42.

[275] *Id.* ¶¶ 38, 43.

[276] Case C-40/17, Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV, EUR-Lex CELEX 62017CJ0040 (July 29, 2019) [hereinafter Fashion ID].

[277] *Id.* ¶ 80.

[278] *Id.* ¶¶ 77–78.

the *Wirtschafsakademie* case*,* the mere consultation of a website featuring the Facebook 'Like' button automatically starts the processing of personal data.[279]

Consequently, the administrator has the obligation to request the consent of the interested party and to provide the pertinent information regarding these specific operations.[280] By contrast, with respect to the phases before or after data collection and transmission, the administrator of the website cannot be considered a controller,[281] so the external provider is solely responsible for the processing.

However, Advocate General Bobek cautioned against interpreting the concept of controller or joint controller in a very inclusive way as the CJEU has already done. What in principle serves to secure the effective protection of personal data, it can become an unfair situation. Thus, when the allocation of liability does not correspond to any control over the result, it "will typically be seen as unreasonable or unjust."[282] If not an exact match, it seems appropriate an adequate connection between control and liability. Or in the terms of Advocate General Bobek, "there ought to be . . . at least a reasonable correlation between power, control, and responsibility."[283] In fact, it has been highlighted that given the configuration of the relations between website administrators and the social network, how it has promoted the insertion of the button in question, and the existing imbalance on many occasions, the result of the judgment implies important obligations and responsibilities for website administrators, that can be especially burdensome for the administrators of certain websites.[284]

In the context of blockchain, the risk increases because following the recent case law, the mere choice of a Distributed Ledger Technology (DLT) to process data may trigger that the user can be considered a controller, without any need to have control over the purposes and the means of processing. Moreover, with the objective of ensuring an effective protection of data subjects, is this protection not really decreasing when every user of a blockchain is made responsible for it? The broad interpretation of joint-controllership presents an additional risk, which is becoming very difficult of delineating spheres of responsibilities. How are we going to ensure that

---

[279] *Id.* ¶ 83.

[280] *Id.* ¶¶ 101–102.

[281] *Id.* ¶ 76.

[282] Opinion of Advocate General Bobek, delivered on December 19, 2019, C-40/17, *Fashion ID*, ¶ 91.

[283] *Id.*

[284] Pedro A. De Miguel Asensio, *El botón "me gusta": aspectos legales*, PEDRO DE MIGUEL ASENSIO (Sept. 9, 2019), http://pedrodemiguelasensio.blogspot.com/2019/09/el-boton-me-gusta-aspectos-legales.html.

making everyone responsible does not mean that no-one will be responsible in fact?[285] The Article 29 Working Party stressed that not being able to directly fulfil all controller's obligations does not exclude one from being a controller.[286] Therefore, in any case a controller will remain ultimately responsible for its obligations and liable for any breach to them, regardless of the inability to fulfill them with the additional danger of hiding responsibilities if a number of people are held responsible.[287] Indeed, the result in such an unclear situation is the opposite of an effective and complete protection of data subjects' rights. The handicap is that nodes cannot see personal data because they are encrypted and hashed. Thus, nodes eventually qualified as controllers may not be able to fulfill the attached obligations and satisfy the rights of data subjects, such as giving a copy of the underlying personal data requested under the right of access.[288]

Furthermore, the European Parliament suggests that "blockchain users may be both data controllers, for the personal data that they upload onto the ledger, and data processors, by virtue of storing a full copy of the ledger on their own computer."[289] However, would it be reasonable that anyone that choses a DLT to process data can be categorized as controller, without any need to have control over the purposes and the means of processing? If the "mere fact of making use of a social network such as Facebook does not make a Facebook user a controller jointly responsible for the processing of personal data by that network,"[290] by analogy a user of the blockchain platform that does not have the tools to influence the network should not be considered a controller. But joint responsibility does not necessarily imply that the various operators have an equivalent responsibility with respect to the same processing of personal data. On the contrary, agents may be involved in different stages of treatment and in various degrees, so that the level of responsibility for each of them must be assessed considering all

---

[285] Anonymisation Techniques, *supra* note 183, at 24 ("[T]he multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing.").

[286] *Id.* at 22 ("First of all, it should be pointed out that, especially in cases of joint control, not being able to directly fulfil all controller's obligations (ensuring information, right of access, etc) does not exclude being a controller. It may be that in practice those obligations could easily be fulfilled by other parties, which are sometimes closer to the data subject, on the controller's behalf. However, a controller will remain in any case ultimately responsible for its obligations and liable for any breach to them.")

[287] Finck, *supra* note 27, at 53–54.

[288] GDPR, *supra* note 10, art. 15.

[289] *Report of the Committee on International Trade on Blockchain: a forward-looking trade policy*, ¶ 23 (Nov. 27, 2018), https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.pdf [hereinafter E.U. Blockchain Report].

[290] Wirtschaftsakademie, *supra* note 273, ¶ 35.

relevant circumstances of the specific case.[291] Thus, if it is argued that no one controls the data, as everyone controls the data,[292] and that more than half of the computing power can change the rules of the blockchain network, then a simple user is going to be a controller of blockchain, following the broad interpretation of joint-controllership by the CJEU.

Overall, the objective to find an effective data protection conversely would risk defending legal rights in an increasing uncertain environment, because of the result of having potentially everyone liable of compliance with data protection rules when power imbalance among actors exists.[293] Considering a user as controller for third-party personal data on a public blockchain may not seem reasonable when personal transaction data is replicated in multiple copies stored on hardware of different users. Therefore, an entity must be provided to enable the reception of requests or claims by the affected data subjects in order to access, modify or delete their personal data. Without *de facto* control, obligations such as those described by the GDPR are meaningless, because it is very onerous demanding users to comply with them, in particular, if they are natural persons.

VI. ALLOCATION OF RESPONSIBILITY TO PARTICIPANTS

A. Tension with the right to erasure

Both the right to rectification[294] and the right to erasure[295] form part of the basic rights of data protection. If blockchain can embrace the right to erasure, we do not see any problem in addressing the right to rectification. This analysis will focus on the right to erasure, but the conclusion can also be applied to the right to rectification.

A commentator states that GDPR terms prohibit using personal data on a blockchain, because the information once entered on a blockchain it is not erasable.[296] As a result, it is necessary to rely on old versions of storing data,

---

[291] *Id.* ¶ 43. Case C-25/17, Proceedings brought by Tietosuojavaltuutettu, 2018 EUR-Lex CELEX 62017CJ0025, ¶ 66 (July 10, 2018).

[292] Daniel Cooper & Gemma Nash, *Blockchain and Privacy*, *in* FINTECH, LAW AND REGULATION 249 (Jelena Madir ed., 2019).

[293] For a similar view on the consequences of a far-reaching interpretation of joint data control, see Renée Mahieu, et al., *Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe*, 10 J. OF INTELL. PROP., INFO. TECH. AND E-COMMERCE L. 84, 94 (2019).

[294] GDPR, *supra* note 10, art. 16.

[295] *Id.* art. 17.

[296] Andries Van Humbeeck, *The Blockchain-GDPR Paradox*, MEDIUM (Nov. 21, 2017), https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047 ("[W]e cannot store personal data directly on the blockchain since in GDPR terms 'it is not erasable'.").

mainly off chain and unfortunately, this technology will not reach its full potential.

First, the assertion that blockchain is immutable is debatable, or at least misleading.[297] The reason is that the ledger is not immutable from a technical point of view. It is possible that nodes achieve consensus to correct local versions of the ledger or revoke past transactions. The difficulty stems from the configuration of the blockchain. Nodes may agree to force a fork, changing the protocol to create a new version of the blockchain. However, it is only considered suitable in specific circumstances. On public and permissionless blockchain cooperation of more than half of the nodes is necessary, which is inevitably costly and not a straightforward manner to correct a record on a register.

The right to erasure is important for the effective application of data protection principles, in particular, the principle of data minimization. According to the data minimization principle, data processing must be limited to what is necessary to fulfil a legitimate purpose.[298] The right to erasure often called the "right to be forgotten" enshrined in article 17 of the GDPR is derived from the fundamental right to data protection.[299] The right to be forgotten consists of the right to delete or cancel personal data connected to past events that may affect free personal development or even human dignity of the data subject. The controller is the person in charge of erasing personal data without undue delay on several grounds. As a result, any problem to identify a controller will affect the option of data subjects to enforce their rights under the GDPR, such as the possibility to direct a complaint to them.

The consistency of data protection as a fundamental right incorporates the need to give full effect to the data subject's rights which is translated in the implementation of de-listing decisions in such a way that they guarantee the effective and complete protection of data subjects' rights. The option of skirting E.U. law should not be a possibility. Therefore, the Working Party guidelines seem to adopt a worldwide approach in relation to the

---

[297] Angela Walch, Blockchain's treacherous vocabulary: one more challenge for regulators, 21 J. OF INTERNET L. 1, 1 (2017) ("[R]ather than being an inherent characteristic, "immutability" of blockchain records is a matter of debate, as high-profile events in the blockchain space have shown that blockchain records are changeable at will by the people who comprise the blockchain system, and it currently is unclear which variations of blockchain technology actually create a record that even approaches immutability."). *See also id.* at 10–16; Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 REV. OF BANKING AND FIN. L. 713 (2016); Gideon Greenspan, *The Blockchain Immutability Myth*, COINDESK (May 9, 2017), *http://www.coindesk.com/blockchain-immutability-myth/* ("In blockchains, there is no such thing as perfect immutability.").

[298] GDPR, *supra* note 10, art. 5(1)(c).

[299] *See id.* art. 17.

implementation of the right to be forgotten, when considering the internet and domain names. It was recognized that de-listing should also be effective on all relevant domains, including ".com" and not only on national domains.[300] In spite of the recognition of the right to data protection to "everyone" laid down in article 8 of the EUCFR, which could mean no actual correlation to the European Union, in practice, the Article 29 Working party specifies that data protection authorities will focus on claims where there is a clear link between the data subject and the Union, for instance, where the data subject is a citizen or resident of an E.U. Member State.[301] Hence, the explicit reference to everyone is modulated to data subjects with an evident connection to the European Union, limiting *de facto* protection to E.U. citizens or residents of a Member State. The scope of certain data protection rights has been very controversial, in particular, the right to be forgotten.[302] In the landmark *Google Spain* decision, the court did not specify the territorial scope of the measures related to the erasure of personal data, which arose as an important aspect considering the diverging views outside the European Union, and notably, in the United States.[303]

Recently, in its preliminary ruling on the *Google LLC* case,[304] the CJEU addressed the question of whether the right to de-referencing must be carried out on a worldwide basis, with regard to all domain names used by its search engine or within the European Union, only on the domain versions corresponding to all Member States; or instead only with respect to the State of residence of the person benefiting from the "right to de-referencing."[305] The court opted for a reasonable and prudent solution, answering the questions jointly. The ruling limits the territorial scope of the right to be forgotten, insofar as search engines are obliged to eliminate in principle the results not worldwide, but in the versions that correspond to the Member States of the European Union, combining it with geolocation mechanisms

---

[300]Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-312/12, 14/EN WP 225, at 3 (Nov. 26, 2014) [hereinafter Guidelines on Implementing Google Spain Judgment].

[301] *Id.* ¶ 19.

[302] Brendan Van Alsenoy & Marieke Koekkoek, *Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'*, 5 INT'L DATA PRIVACY L. 105, 110 (2015).

[303] However, some claim that Americans deserve a right to be forgotten. Joseph Steinberg, *Why Americans need and deserve the Right to be Forgotten*, INC. (Feb. 7, 2018), https://www.inc.com/joseph-steinberg/why-americans-need-deserve-right-to-be-forgotten.html; Erin Cooper, *Following in The European Union's Footsteps: Why The United States Should Adopt its Own "Right To Be Forgotten" Law for Crime Victims*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 185 (2016).

[304] *See* Google LLC, *supra* note 143.

[305] *See id.*

that have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question from the territory of the Union.[306]

The last ruling further elaborates a rationale on how de-listing the links worldwide would meet the objective of guaranteeing a high level of personal data protection throughout the European Union in full, since the Internet is a global network and listing a link with information referring to a person located in the European Union is "likely to have immediate and substantial effects on that person within the Union itself."[307]

Nevertheless, four arguments support the decision against extending de-listing worldwide. One argument is a factual issue, considering the state of the law from a global perspective; notably, the actual divergence on the right to de-listing in different States, as far as it is not a right in some States. The second argument is based on the data protection right. Although it has the status of a fundamental right, it is not absolute, which obliges to strike a balance "against other fundamental rights, in accordance with the principle of proportionality."[308] The third argument is founded on the lack of intention of the European legislature to extend rights beyond the territory of the European Union related to a textual interpretation of the Directive and the GDPR.[309] Finally, a cooperation mechanism for supervisory authorities does not exist with regard to the scope of de-referencing of links outside the Union in contrast with the right to have access to information.[310]

In addition, the court emphasized that E.U. law does neither require that de-referencing in all versions of the search engine in question, nor prohibit such a practice. This ruling can open a door for uncertainty because a supervisory or judicial authority of a Member State is competent to balance the protection of personal data with the right to freedom of information and after an analysis on a case-by-case basis, the national authority can oblige the operator of a search engine to de-referencing in all versions of that search engine.[311] Yet, this interpretation is consistent with article 85 of the GDPR that enables Member States to enact laws in order to reconcile the right to the protection of personal data with the right to the protection to freedom of expression and information.[312] As a result, national standards that weigh up the accommodation of two fundamental rights do not have to be uniform.

---

[306] *Id.* ¶ 53–54.
[307] *Id.* ¶ 55–57.
[308] *Id.* ¶ 60.
[309] *Id.* ¶ 62.
[310] Google LLC, supra note 143, ¶ 63.
[311] *Id.* ¶ 72.
[312] *See* GDPR, *supra* note 10, art. 85.

However, the problematic question is how to interpret the right to erasure and modification within the framework of blockchain. Considering that in the absence of trust, blockchain's will is to enhance data integrity, not allowing to modify or erase data once entered on the blockchain. By an orthodox definition, "a ledger is a database which keeps a final and definitive record of transactions."[313] In other words, DLT is tamperproof or deliberated designed to avoid a modification. Thus, records, once stored, cannot be modified without leaving behind a mark.

To solve the tension between blockchain and the right to erasure, the options vary from the most permissible to the most orthodox. Should we make an exception in order to feed and promote the potentialities of blockchain? Or on the contrary should we read strictly the GDPR and conclude that if personal data entered in the blockchain cannot be erased or modified, this technology should not be put in place, at least on a broad scale.[314] The European Parliament recommended that "blockchain technology should not be used for the processing of personal data until the user [organization] concerned is in a position to guarantee compliance with the GDPR and to specifically ensure that the rights to the rectification and erasure of data are protected."[315] However, this can become an obstacle of innovation, stifling our technological future, lagging behind the most technological nations. It seems that the European Union is doing precisely the opposite, for example, multiple initiatives are currently researching how it would be possible to apply blockchain to public services.[316]

B. Proposed Solutions

An alternative to a strict interpretation of a complete elimination of the data may be to limit the processing by inspiration in some laws of the Member States. Some national laws do not oblige to delete the data when it is not possible in the case of non-automated processing in a specific way of storage.[317] Since not all national laws allow such possibility, for instance,

---

[313] Patrick Van Eecke & Anne-Gabrielle Hair, *Blockchain and the GDPR: The EU Blockchain Observatory Report*, 4 EUR. DATA PROT. L. REV. 531, 531 (2018).

[314] David Meyer, *Blockchain technology is on a collision course with EU privacy law*, IAPP (Feb. 27, 2018), https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

[315] E.U. Blockchain Report, *supra* note 289, ¶ 22.

[316] *See generally* David Allessie et al., *Blockchain for digital government*, JOINUP (2019), https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (the initiatives include the Exonum land title registry, Blockcerts academic credentials, Chromaway property transactions, uPort decentralized identity, Infrachain governance framework, Pension infraestructre, and Stadjerspass smart vouchers.).

[317] *See* Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, June 30, 2017, art. 35 (Ger.).

Spanish law containing the right to erasure refers to article 17 of the GDPR,[318] this interpretation could hamper the original objective of the regulation, which is to avoid the fragmentation of the applicable law within the European Union. However, the GDPR does not provide a full exhaustion of powers by Member States. Indeed, some provisions set out that Member States are allowed to determine certain aspects, for instance, the age to consent in minors[319] or the setting or national standards to reconcile the right to data protection with other fundamental rights.[320] Therefore, the alternatives to the right to erasure could be set for in a not uniform manner across the Member States. This situation may not be optimal, but can be a temporary result until the European Data Protection Board (EDPB) develops guidelines for all Member States in the future. One interpretation is considering that an exemption exists because of technical blockchain technology limitations. Article 17(2) of the GDPR refers to the "account of available technology and the cost of implementation" when the data controller has to answer to a request for erasure.[321] However, specific technological advances like an editable blockchain could help to limit the problem, where in the end depends on having computing power to reverse the situation.[322]

A reinterpretation of the concept of erasure, by softening it, could allow that specific technological techniques that "hide" personal data can comply with the right to be forgotten. For instance, the chameleon hashes allow to edit, remove or rewrite certain data. Against this approach, concern related to denature blockchain appears since it will be necessary a trusted body to judge where it is necessary to edit the blockchain.[323] Apparently, the solution does not eliminate the risk of miners not willing to comply with the orders of the trusted body and the old copies remain in the blockchain infrastructure, in particular, where miners are located abroad. Indeed, they tend to locate in certain parts of the world usually benefiting of lower electricity costs, where there is the highest concentration of hardware. The great example is Bitcoin and the concentration of miners in large areas (mining fields) as a new form of investment in China or in the United

---

[318] *See* Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales art. 15 (B.O.E. 2018, 294) (Spain).
[319] GDPR, *supra* note 10, art. 8.
[320] *Id.* art. 85.
[321] *Id.* art. 17(2).
[322] Daniel Conte de Leon et al., *Blockchain: Properties and Misconceptions*, 11 ASIA PAC. J. OF INNOVATION & ENTREPRENEURSHIP 286 (2017).
[323] Giuseppe Ateniese et al*., Redactable Blockchain or Rewriting History in Bitcoin and Friends*, INT'L ASS'N FOR CRYPTOLOGIC RES. (May 11, 2017), https://eprint.iacr.org/2016/757.pdf.

States.[324] This means that the "volunteers" (servants of the infrastructure) that make it work may not be encouraged to comply with European privacy legislation on personal data stored in the blockchain, maybe because it is costly to implement several of the solutions that can mitigate the exposure of personal data in blockchain. In addition, such dependence with countries whose standards are different can make public and permissionless blockchain not developing at the expected speed, precisely because the entities that can make use of the new technology do not trust that their data will be safe through nodes that are outside the borders of the European Union.

In our opinion, making data inaccessible on a blockchain could be equivalent to erasure in a similar way that de-listing in a search engine has not to be deployed worldwide based on the *Google LLC* case.[325] This could be assimilated to what happens in social networks when an operator is obligated to comply with a request for erasure at the source; but this does not (necessarily) lead to a complete erasure because once content has been shared on the social network, third parties might not be subject to European data protection law.[326] Applying this reasoning to blockchain, a copy stored on a node might be "erased" (in the sense of making inaccessible), but nodes not subject to European jurisdiction could still have a copy of that personal data. This would lead to a smart enforcement of data protection rules. Moreover, making data inaccessible could be reached using different techniques. One could be the destruction of the private key[327] and another using pruning techniques for the purpose of removing the personal data at issue.[328]

Another possible scenario is that exemptions to the right to be forgotten may be applicable. Perhaps the most significant one may be to comply with a legal obligation, because the law of the European Union or a Member State so dictates by virtue of article 17(3)(b) of the GDPR.[329] This can be the case

---

[324] For an interesting example of a Chinese owner building a mining field in the United States, see Bradley Keoun, *Why Bitmain is Building the World's Largest Bitcoin Mine in Rural Texas*, COINDESK (October 22, 2019), https://www.coindesk.com/why-bitmain-is-building-the-worlds-largest-bitcoin-mine-in-rural-texas.

[325] Google LLC, *supra* note 143. For a background on this judgement, see Guidelines on Implementing Google Spain Judgement, *supra* note 300, at 3 ("[L]imiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment.").

[326] LUKAS FEILER, NIKOLAUS FORGÓ & MICHAELA WEIGL, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A COMMENTARY 121 (2018).

[327] CNIL, *supra* note 184, § 8.

[328] EUR. UNION BLOCKCHAIN OBSERVATORY AND F., *supra* note 38, at 31.

[329] *See* GDPR, *supra* note 10, art. 17(3)(b).

of storing personal data due to "national commercial or tax law."[330] Therefore, compliance with legal obligations can be an exception of the right to be forgotten also in the blockchain context.

Faced with a mistake or a hacker attack, it has been experienced how the community has reacted and adapted to the circumstances. The DAO has exemplified a real situation of how the effects of a hacking can be reversed. In the case the hacker exploited a weakness of the Ethereum software, so that part of the DAO funds in Ether went to the hacker account. Fortunately, a fork was conceived to return all the Ether taken from the DAO to refund a smart contract. Investors could receive 1 ETH for every 100 DAO, in other words, changes of the protocol were allowed. Supporters of reversing the situation consider that human beings should have the final decision through social consensus.[331] The decision was taken by a qualified majority of 89%.[332] Since 2016, Ethereum split into two chains, the main Ethereum chain (ETH) and the Ethereum classic (ETC). Hence, technology through a hard fork that represents a change in a protocol was used to plow back an unjustified situation. Those who opposed to change the protocol gave grounds for maintaining the essence of blockchain immutability and at the same time the core part of a smart contract, basically no need for human hand for execution of the contract.

However, it could be understood that a protocol is not independent from the community that support and feed it. When the community agrees to change the protocol, if this is adopted via consensus of the decentralized community and to address a present and clear danger to its network, it seems to be justified.[333] Thus, if the organization does not want an immutable ledger, why should the technology constraint it?

In reality, technology is the result of a human mind. The use of blockchain cannot be operative outside the law. In the same way that Internet development was influenced by geographical borders because "Internet users around the globe demanded different Internet experiences that corresponded to geography,"[334] and not only as a result of national governments, companies and entities will adapt blockchain technologies to their structural necessities. For public records of property or insolvency companies,

---

[330] PAUL VOIGT & FREIHERR AXEL VON DEM BUSSCHE, THE EU GENERAL DATA PROTECTION REGULATION (GDPR): A PRACTICAL GUIDE 160 (2017).

[331] Antonio Madeira, *The Dao, the Hack, the Soft Fork and the Hard Fork*, CRYPTOCOMPARE (Mar. 12, 2019), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/.

[332] *Id.*

[333] *See* Dominik Williams, *Hard fork Ethereum to revert the hack of the DAO*, CHANGE.ORG (2016), https://www.change.org/p/ethereum-hard-fork-ethereum-to-revert-the-hack-of-the-dao.

[334] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 49 (2006).

blockchain can provide a new way of managing and registering them as legal persons do not enjoy the right to data protection; whereas for other purposes and applications of blockchain like smart contracts, parties will tackle the challenges of using an execution of the contract that carries out automatically and where it is not possible to address supervening changes of circumstances. Therefore, the immutability of the ledger shall need to adapt to the will of the parties or may not be an effective alternative to execute a complex contract.

Similar to the experience of the internet, which at the beginning it was considered an anarchic space, but now it is regulated specially on intermediaries' actions and liabilities, blockchain technologies are raising the awareness of governments. Governments' interests will be shaped on the blockchain technology with the intention to control it, but private actors will also modulate the emerging technology to satisfy their needs and accommodate differences among users and regions. Developments with encryption will allow gaining trust in the blockchain from a data protection perspective, when privacy enhancing technologies gain prevalence in the market as they can specifically be designed to comply with existing regulations.[335] The challenge of decentralization based on blockchain will be limited insofar as private actors tailor it to their interests pushed by efficiency and storage concerns.

VII. SOME RECOMMENDATIONS AND TRADE-OFFS

A multi-pronged strategy would be appropriate to address the tension between blockchains and GDPR. The privacy by design principle is enshrined in article 25 of the GDPR.[336] Privacy by design of blockchain applications could be possible through different mechanisms. The use of storing data off-chain mechanisms, encryption, hash functions, noise adding, ring signatures, an editable blockchain, non-interactive zero-knowledge proofs are some techniques that can be embedded in blockchain applications to comply with the GDPR.

A. Storing data off-chain mechanisms

A division of data storage can be a plausible solution to confront many challenges, in particular, not all data has to be in the blockchain itself. Basically, the designer of the blockchain can envision a different way to data storage. Personal data can be stored on a database that is not integrated in

---

[335] *See* David Harborth et al., *Integrating Privacy-Enhancing Technologies into the Internet Infrastructure*, UNIVERSITÄT REGENSBURG (2016), https://epub.uni-regensburg.de/36346/1/description_english.pdf.
[336] *See* GDPR, *supra* note 10, art. 25.

the chain, rather it is linked to the distributed ledger via a hash. The problem of classifying data as personal data is not solved by this technique, but once it is clear which data is deemed personal data, the recommendation is to keep them off-chain.[337] The first solution could be not storing personal data in a blockchain. For instance, when users of a blockchain are businesses, legal persons, the platform could be configured in a permissioned manner to reflect the settlement of interbank payments. As a result, a consolidated amount of any bank would appear in the blockchain, avoiding storing individual transactions.

However, some issues arise given that a possible solution to keep transactional data in an off-chain data base cannot be applied to public keys. The second concern is a philosophical question that limits the potential benefit of using blockchain as a single and shared source of truth.[338] Inevitably, the use of data storage in off-chain databases multiply the number of records. Yet, this fact by itself is not a disadvantage from a security perspective; because when data are stored in different records is less likely that all records to be manipulated if compared to data stored on a centralized secure ledger. Likewise, despite data is not kept in the ledger, a hash pointer remains in the ledger, which raises doubts about how it ought to be managed when the original personal data is rectified or erased.[339]

In addition, limiting ledger storage has been proposed as a privacy-by-design solution.[340] The idea is to store the entire ledger on one (or a few) instances only, and to instruct all other nodes to delete the information on a new block after verification has taken place. Therefore, two sources could be consulted for verification purposes: the full ledger and the nodes maintaining the verification purposes. Indeed, this solution could enable data subjects to enforce their rights.

---

[337] Matthias Berberich & Malgorzata Steiner, *Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers*, 2 EUR. DATA PROT. L. REV. 422, 425 (2016).

[338] *A guide to blockchain and data protection*, HOGAN LOVELLS ENGAGE 18 (2018), https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf.

[339] Finck, *supra* note 27, at 32.

[340] Moerel, *supra* note 222, at 847 ("A privacy-by-design solution would be to store the entire ledger on one (or a few) instances only, and to instruct all other nodes to delete the information on a new block after verification has taken place. This will still enable the nodes to fulfil their verification function, while at the same time the full ledger can still be consulted if so required for verification purposes. This change in design will not only limit the storage of personal data and increase confidentiality, but also has economic advantages, such as saving storage capacity and energy consumption.").

B. Security Mechanisms: encryption and hashes functions

Anonymous data can be difficult to delineate from pseudo-anonymous data. Encryption and hash functions are commonly used to provide a robust security to personal data and it is often misunderstood that through them data become anonymous. Far from the reality in most situations, encryption and hashing techniques could not irreversibly produce anonymous data. First, encryption works using a key. Whenever someone knows the key to decrypt, personal data is still plain, so for the holder of the key, encrypted data is always personal data. Second, hash functions are deterministic and operates in a way that the same input always yields the same output. A computer can solve the puzzle trying with different dataset, for example, email addresses, names and social security numbers to check if the output (what hash is revealed) coincides with a previously known output. Therefore, linking between the two sets of data reveals that hashing does not transform personal data in anonymous data. In principle, output data remain personal data as it keeps to be pseudonymous, that is to say that with additional information, it is possible to personalize pseudonymous data. Some kind of hash, as salted hash and keyed hashes have been considered by the Article 29 Working Party.[341] Despite being methods that reduce the likelihood of deriving the input value, it does not make impossible finding the input value.

Following a risk-based approach would make hash functions, even the one with stronger privacy guarantees, not able to convert personal data in anonymous data under GDPR.[342] It is well-known, that using backdoors or master keys makes possible to decrypt every message in an encrypted software, but having access to that knowledge is not widespread. It is a remarkable example that law enforcement agencies ought to use their specific powers to target and investigate criminals without requiring developers access to backdoors or master keys in a general manner.[343] This uncertainty regarding anonymization techniques spreads over blockchain technologies, being possible to unveil personal data through re-personalisation, when that supposedly was secure enough and immune to it.

However, some have advocated to focus on who has the key access. In Cloud Computing, if the provider has no key access, data are deemed to be sufficiently well-encrypted data, and therefore, they ought not to be personal data.[344] It seems reasonable to assess whether anonymous data could be re-

---

[341] Anonymisation Techniques, *supra* note 183, at 20.

[342] *See supra* § IV.B for a description of a risk-based approach.

[343] *See* Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU, 14/EN WP 221 (Apr. 11, 2018).

[344] W. Kuan Hon, Christopher Millard & Ian Walden, *Who is Responsible for `Personal Data'*

converted in personal data. In our opinion, this analysis must be done vis-à-vis a specific person, such as the data controller. In the opposite case, framing an absolute approach, taking into consideration anyone who may be able to identify a data subject, could be a very broad definition, as rendering impossible to examine if any third party is not capable to unveiling a person identity. In fact, the Article 29 Working Party has recognized this issue as "a very significant grey area."[345]

The absolute perspective can be considered to protect effectively data subjects in light of data protection as a fundamental right. For academics in favor of protecting personal data, de-encryption must be considered from the point of view of data controllers and third parties, justifying this interpretation on the wording of GDPR recital 26 ("by the controller or by another party.").[346] Nevertheless, from a practical point of view, this may be very burdensome to implement. Considering an absolutist approach correct would lead to examine anyone who was able to identify a person in blockchain. For example, a third party can have no relation with the data subject or even without being a user of the blockchain itself, but may be capable of re-identify personal data, in particular, on public and permissionless blockchains.

C. Available techniques to pursue anonymity

Some kind of data, such as health data or census data is mostly public or semi-public and some basic characteristics (eg. ZIP code, gender, date of birth) may likely identify persons.[347] The addition of noise consists of altering attributes by adding or removing a different random value for each record.[348] According to the Article 29 Working Party, adding noise may be an acceptable anonymization technique.[349] While adding noise to data as a perturbation technique enhances privacy, the trade-off is shrinking data utility, that is how useful a published dataset is to the consumer.[350]

---

in Cloud Computing? The Cloud of Unknowing, *Part 2* 18 (Queen Mary Sch. of Law Legal Studies Research Paper No. 77/2011, 2011).

[345] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, at 31, 00569/13/EN WP 203 (Apr. 2, 2013).

[346] Buocz et al., *supra* note 237, at 190.

[347] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* (Carnegie Mellon Univ. Data Privacy Working Paper No. 3, 2000), https://dataprivacylab.org/projects/identifiability/paper1.pdf.

[348] Mohammed J. Khan, *Big Data Deidentification, Reidentification and Anonymization*, ISACA J. (Jan. 1, 2018), https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/big-data-deidentification-reidentification-and-anonymization.aspx.

[349] Anonymisation Techniques, *supra* note 183, at 12–13.

[350] Kato Mivule, *Utilizing Noise Addition for Data Privacy, an Overview*, CORNELL U. ARXIV (Sept. 16, 2013), https://arxiv.org/pdf/1309.3958.pdf.

Second, the technique called "multi-layered linkable spontaneous anonymous group" allows to hide the origin, destination and amount of transactions.[351] This is based on digital signature which specifies a group of possible signers, but the verifier cannot tell which member actually produced the signature.

Third, editable blockchain permits exactly the modification of past blocks, changing the way hash pointers link blocks.[352] Editable blockchains are becoming a feasible option, as some researchers state that implementing a redactable blockchain requires only minor modifications to the current structure of the blocks.[353] Thus, it appears that this possibility could be used in privacy-by-design applications. This would facilitate the exercise of fundamental rights, in particular, the right to be forgotten, that was the most technically controversial on a blockchain technology. Nevertheless, the implementation of editable blockchains would require the appointment of administrators to alter the ledger.

Fourth, merge avoidance tries to minimize the number of times that you link accounts together by spending from them at the same time. However, it is not a definite solution for privacy concerns.[354]

Fifth, non-interactive zero-knowledge proofs use protocols where it is not necessary that a prover and verifier are present during the execution of the protocol. The prover generates a statement and the verifier can check its validity later. It can be used to prove that someone is not a minor, without providing personal data, such as your name, address or photos. Examples of zero-knowledge protocols are implemented already in some cryptocurrencies like Zcash and Zerocoin.[355] These systems overcome the public exposure of sensitive data by entering into Bitcoin transactions.[356] New cryptocurrencies offer stronger privacy, because it is only visible that a transaction has been made, without disclosing public keys, amounts or sender and recipient information. In this sense, they overcome deficits of Bitcoin, altering what is recorded in the distributed ledger. However, it is worth noting that "as with mixing systems, these techniques may only hide payees within a limited list

---

[351] Shen Noether, *Ring Signature Confidential Transactions for Monero*, INT'L ASS'N FOR CRYPTOLOGIC RES. (2015), https://eprint.iacr.org/2015/1098.pdf.

[352] *See* Richard Lumb et al., *Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world,* ACCENTURE (2016), newsroom.accenture.com/content/1101/files/Cross-FSBC.pdf.

[353] *See* Ateniese et al*., supra* note 323.

[354] Buterin, *supra* note 90.

[355] Ian Miers et al., *Zerocoin: Anonymous Distributed E-cash from Bitcoin*, ZEROCOIN PROJECT, http://zerocoin.org/media/pdf/ZerocoinOakland.pdf

[356] Mike Hearn, *Merge avoidance, A note on privacy-enhancing techniques in the Bitcoin protocol*, MEDIUM (Dec. 11, 2013), https://medium.com/@octskyward/merge-avoidance-7f95a386692f.

of potential users, not all, which opens the way to de-anonymizing multiple transactions."[357] In spite of this inconvenience, the European Parliament encourages to fund academic research to conclude whether zero knowledge proofs could be a way to comply by design with the data protection requirements.[358]

D. Negative consequences of anonymity

Techniques to achieve anonymity solve a problem with regard to data protection law. However, pursuing anonymity in blockchain transactions can have negative consequences until the point of compromising the integrity of markets, the protection of investors and consumers, and even economic and financial stability of a given country. One of the criticisms of anonymous cryptocurrencies is that they can be used to finance illegal activities[359] or even avoid economic sanctions against hostile countries, to such an extent that they could pose national security risks.[360]

Some national governments have prohibited the use of cryptocurrencies in the name of national interest, as well as techniques that prevent access to underlying transaction data such as origin, destination and amount exchanged.[361]

The following example illustrates how an asset that complies with basic principles of data protection is not excluding of suffering devastating consequences because of the characteristic of anonymity. Monero, which

---

[357] GOVERNMENT OFFICE FOR SCIENCE, DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, 2016 (UK), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. at 51.

[358] E.U. Blockchain Report, *supra* note 282, ¶ 21.

[359] *Serious and Organised Crime Threat Assessment (SOCTA)*, EUROPOL 34 (2017), https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

[360] *See Cryptocurrency and national security*, THE HARVARD GAZETTE (Nov. 20, 2019), https://news.harvard.edu/gazette/story/2019/11/crisis-simulation-maps-national-security-risks-of-digital-currency/?utm_source=SilverpopMailing&utm_medium=email&utm_campaign=Daily%2520Gazette%252020191121%2520%281%29 (discussing a simulation that took place at the Harvard Kennedy School with academics and officials about taking action against a crisis caused by cryptocurrencies and that would affect the national security in the United States through cyberattacks on individual banks and the international SWIFT banking network.).

[361] *See* Resolucion de Directorio nº 044/2014, BANCO CENTRAL DE BOLIVIA (May 6, 2016), https://www.bcb.gob.bo/webdocs/01_resoluciones/044%202014.PDF. In Colombia, although there is no specific law banning cryptocurrencies, financial institutions are not authorized to guard, invest, mediate or operate with these instruments. *See also Carta Circular 52 de 2017*, SUPERINTENDENCIA FINANCIERA DE COLOMBIA (June 22, 2017), https://www.superfinanciera.gov.co/jsp/10089581#_ftn2.

uses the Cryptonote protocol, is one of the most protective cryptocurrencies for privacy.[362] Cryptonote is based on an encryption system that requires transactions to not just signed by a single person, but by several at once.[363] For this, the system divides the amount of Moneros into two (unequal) parts and mixes both with the Moneros of other users. In the end, it obfuscates, mixes everything to make the transfers in such a way that it is impossible to know the origin of the funds and which is the destination. The advantage of this protocol is that Monero transactions are not linkable or traceable, that is, it offers total anonymity to users.

However, its advantage is the source of the withdrawal of the cryptocurrency from particular markets, since BitBay, based in Estonia, will not trade with this cryptocurrency as from February 19, 2020.[364] It is not the first crypto exchange that proposed to exclude privacy-oriented currencies. In September 2019, Upbit, based in South Korea, removed support for several cryptocurrencies including Monero and Zcash.[365] Some argue that if a cryptocurrency remains viable, such as Bitcoin, it is due to the possibility to know the origin of the money comparing it with Monero or Zcash.[366] Yet, one of the risks of using Bitcoin is namely the lack of privacy, for instance, if someone mistakenly shares his Bitcoin address, anyone can check his balance and the other addresses with which he has interacted; it can be assimilated to give the password of your online banking details, with the difference that banks usually add different kinds of security layers. As a result, it seems more a firm decision links to the illegal use of the cryptocurrency, which prevents the use by people who are not criminals and who legitimately do not want to reveal how much money they have.

Virtual currencies can have a certain degree of anonymity as the dropping of the statement "virtual currencies cannot be anonymous," from the proposal on the definition of virtual currencies in a European Council Directive reveals.[367] Therefore, prohibiting a private cryptocurrency under the law can be an ineffective policy, because technology will try to develop techniques to overcome the law.

---

[362] *Monero: The Only True Privacy Coin?*, TRADING EDUCATION (Feb. 10, 2020), https://trading-education.com/monero-the-only-true-privacy-coin.

[363] *Id.*

[364] Daniel Palmer, *Another Crypto Exchange Is Dropping Privacy Coin Monero Over Compliance Risk*, COINDESK (Nov. 26, 2019), https://www.coindesk.com/another-crypto-exchange-is-dropping-privacy-coin-monero-over-compliance-risk.

[365] William Foxley, *South Korea's Upbit Becomes Latest Exchange to Delist Privacy Coins*, COINDESK (Sept. 20, 2019, 9:34 PM), https://www.coindesk.com/south-koreas-upbit-becomes-latest-exchange-to-delist-privacy-cryptocurrencies.

[366] Álvaro Hernández, *Monero, la alternativa a Bitcoin que se ha convertido en la divisa de los criminales*, EL DIARIO, (Feb. 9, 2017), https://www.eldiario.es/hojaderouter/internet/monero-criptomoneda-mercado_negro-criminalidad_0_610688987.html.

[367] *See* Council Directive (EU) 2018/843, art. 3(18), 2018 O.J. (L 156) 43,63.

CONCLUSION

There can be no one-size-fits-all legal response. In any case, the use of blockchain is an alternative for every business or organization, not a replacement. It shall be necessary to tailor appropriate legal solutions to each case as outcomes will depend on how the technology is designed. The real value of blockchain technologies lies in facilitating more efficient digital-assets transfers from an economic perspective.[368] As a result, the applications of blockchains have not yet reached their full potential, they can be used not only for cryptocurrencies, but could also revolutionize transactions in other trustless environments. In the private realm, authorship verification, title transfers and contract enforcement could be transformed with blockchains. Public institutions may also decide to implement blockchains in order to manage and run public administration services. For example, they can potentially facilitate the right to vote.

The definition of the blockchain protocol is key to understand the characteristics of the infrastructure (public or private, permissioned or permissionless). The various actors play different roles depending on the characteristics defined at the infrastructural level. It seems appropriate to analyze data protection law from a micro-perspective, in other words, what happens in an individual transaction,[369] in contrast to the macro-perspective. Meanwhile the purpose of processing refers to recording a specific transaction onto a blockchain; the means are deemed to be the choice of the blockchain platform.

Blockchains are under the scope of the GDPR if they have a presence in the European Union that can be considered establishment such having nodes in the European Union; or under the market approach if they are targeting or monitoring data subjects located within the Union. Therefore, many public and permissionless blockchains will be under the scope of the GDPR.

Public keys work as identifiers, so they are personal data under the GDPR. The option of using one-time public keys will minimize the risk of re-identification by singling out, linkability, or inference methods with additional data. Additional data that is contained in the blockchain can be considered personal data when meets the requirement of identifying a person directly or indirectly. The cautious option is to use one-time public keys methods with additional data and to avoid entering personal data on a plain form in a blockchain. Using available encryption techniques will reduce the risks of re-identification by singling out, linkability, or inference methods.

---

[368] *See* Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015).

[369] Bacon et al., *supra* note 29, at 64.

With regards to identifying controller(s) or processor(s), the configuration of a blockchain as private and permissioned could alleviate the difficulty of complying with E.U. law. Yet the identification of controllers in public and permissionless blockchains seems controversial. The relevant aspect is whether nodes and miners are processing personal data taking an active role or a passive role (on behalf of the users). If they adopt a passive role facilitating the transactions, they still should be regarded as processors by analogy with cloud providers. Users will be considered controllers, unless they benefit from the purely domestic exception. However, the users' exemption is read very narrowly by the CJEU. Considering most users of a blockchain controllers will undermine the effectiveness of a full data protection, because users may not know if they are interacting with blockchains that are compliant with data protection law and personal transaction data is replicated in multiple copies stored on hardware of different users. Creating a certification mechanism to determine if a blockchain application is GDPR-compliant could be a solution. However, the lack of *de facto* control by most users will not allow an effective enforcement of individual data protection rights. Therefore, developers should be encouraged to build privacy-by-design blockchain applications. Ruling on specific guidance on privacy-by-design to industry stakeholders may be counterproductive and inimical to new developments.[370] However, privacy considerations should not be left to users alone in specific cases (e-voting) and a privacy-by-design perspective from the organization running the protocol ought to be expected.

Enforcing data subjects' rights on a blockchain is not straightforward. The proposed solution is that the right to erasure must be interpreted in a contextual way. The option of making data inaccessible should qualify as erasure, considering the reasoning of the *Google LLC* case. A copy stored on a node might be inaccessible, but nodes not subject to European jurisdiction could still have a copy of that personal data. Likewise, complying with a legal obligation under another law will exempt the right to erasure as GDPR provides. Moreover, a fork is not unfeasible as a blockchain protocol is not independent from the community that support and feed it. With this technique the modification of personal data is possible.

The use of storing data off-chain mechanisms, encryption, hash functions, noise adding, ring signatures, an editable blockchain and non-interactive zero-knowledge proofs could foster privacy solutions. However, these recommendations involve trade-offs that should be considered in each particular use.

---

[370] Moerel, *supra* note 222, at 851.

In addition, it may seem a paradox to comment on the risks that blockchains entail for privacy and data protection when most of the legal attention paid to cryptocurrencies so far has focused on the risks of their "secret" uses outside the law. Consequently, the greater the privacy protections in the blockchain protocols, the more easily criminals, terrorists, funders of illicit activities and tax evaders can pursue its ends.

However, the distributed nature of the public networks should not serve as an excuse to neglect existing law for the protection of personal data. Protecting personal data for users and ensuring transparency in certain circumstances should be facilitated if required.[371] As professor Zittrain wrote on the future of the internet, but applying it to blockchain: the blockchain's future may be brighter if technology permits easier identification of blockchain users combined with legal processes, and perhaps technical limitations, to ensure that such identification occurs only when good cause exists.[372] Combining the best of both worlds should be the goal of privacy-by-design blockchain networks. Conversely, the policy of prohibiting blockchain technologies because they are too anonymous and can be used for laundering money and financing terrorism should be taken very cautiously. The risk of criminalizing users merely for using blockchain technologies to carry out transactions is enormous. First, the quantity of people using blockchains for legitimate purposes may be increasing.[373] Second, blockchain applications that guarantee anonymity will still be used by dishonest users.

Therefore, researchers should continue to implement public blockchains designs to comply with data protection regulations, because the benefits for mainstream individuals outweigh any potential illegitimate use.

Finally, the evolution of blockchain technologies will mirror the evolution of the Internet itself, whose first users dreamed to decentralize power, but now find it highly regulated and concentrated. It is remarkable

---

[371] *See, e.g.*, GDPR, *supra* note 10, art. 23.1(d) (discussing restrictions on the scope of obligations and rights for data subjects in case of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.); Council Directive (EU) 2016/680, 2016 O.J. (L 119) 89.

[372] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 194 (2008).

[373] The prohibition of Bitcoin in countries like Bolivia does not impede people from using it. *Incluso con la prohibición la población de Bolivia recurre al Mercado paralelo de Bitcoin*, COINTELEGRAPH (Nov. 14, 2019), https://es.cointelegraph.com/news/crise-estaria-levando-populacao-da-bolivia-a-recorrer-ao-mercado-paralelo-de-bitcoin. Likewise, the number of establishments accepting cryptocurrencies in Colombia is increasing despite the alerts from Colombian authorities. *See* Santiago Vásquez Rodríguez, *El escenario normativo tras la irrupción de las criptomonedas en Colombia*, UNIVERSIDAD DEL ROSARIO 11 (2019) https://repository.urosario.edu.co/bitstream/handle/10336/19941/EL%20ESCENARIO%20NORMATIVO%20TRAS%20LA%20IRRUPCIÓN%20DE%20LAS%20CRIPTOMONEDAS%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y.

how we accept in our era the dominance of technology, as if technology were superior to human beings. In this line of reasoning, we cannot forget that "technologies are always economic means, not ends in themselves: in modern times, technology's DNA comes already patterned by what the sociologist Max Weber called the 'economic orientation.'"[374] Power determines technology, selects certain technologies and discards others. Blockchain technology will depend on a given network´s goals and governance arrangements, including privacy concerns.

[374] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 15 (2019).